Deutscher Bundestag **Drucksache 16/4763**

16. Wahlperiode 21. 03. 2007

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz – SatDSiG)

A. Problem und Ziel

In Deutschland entstehen zurzeit sehr leistungsfähige Erdfernerkundungssatelliten mit dem Ziel einer gewerblichen weltweiten Vermarktung der Daten. Die derart entstehenden Daten haben eine Qualität, welche bis vor kurzem nur von klassifizierten militärischen Satelliten erzeugt werden konnte und daher nur innerhalb von militärischen Systemen nutzbar war. Diese Daten sind sicherheitsrelevant: Wirkungen von Waffen oder politische Drohungen können durch diese Erdfernerkundungsdaten erheblich verstärkt werden.

Im deutschen Recht gibt es keine Regelungen, welche das Verbreiten von Daten oder Bildern derartiger Qualität betreffen.

Zudem sind nahezu alle leistungsfähigen Erdbeobachtungssysteme auf US-amerikanische Bauteile angewiesen. Die USA machen eine Exportgenehmigung für diese Bauteile davon abhängig, dass nationale Regelungen bestehen, welche Sicherheitsinteressen bei Erzeugung oder Verbreiten der Erdfernerkundungsdaten berücksichtigen.

Mit dem Gesetz sollen die sicherheits- und außenpolitischen Interessen der Bundesrepublik Deutschland bei dem Verbreiten von Erdfernerkundungsdaten gewahrt werden. Dadurch werden mittelbar auch Rechtssicherheit für betroffene Unternehmen erreicht und die Besetzung der neuen Geschäftsfelder im Geoinformationsmarkt kalkulierbar gemacht.

B. Lösung

Mit dem Gesetz werden die rechtlichen Rahmenbedingungen für eine private Erdfernerkundung und eine weltweite Vermarktung der dabei gewonnenen Daten geschaffen. Im Mittelpunkt der Regelungen des Gesetzes steht eine Prüfung des Inverkehrbringens oder Zugänglichmachens von Erdfernerkundungsdaten und -datenprodukten.

Diese Prüfung wird jedoch nur erforderlich, wenn die Daten mit einem Erdfernerkundungssystem erzeugt worden sind, das technisch in der Lage ist, die Sicherheitsinteressen der Bundesrepublik Deutschland zu gefährden. An den Betrieb solcher hochwertiger Erdfernerkundungssysteme werden Anforderungen gestellt, die verhindern, dass diese von Unbefugten kommandiert oder Daten von Unbefugten eingesehen werden können. Hierzu muss der Betrieb des Erdfernerkundungssystems genehmigt und beaufsichtigt werden.

Die Prüfung des Inverkehrbringens oder Zugänglichmachens erfolgt teilweise durch den Datenanbieter selbst. Indem er diese Prüfung eigenverantwortlich durchführen kann, kann er die Daten ganz überwiegend ohne behördliche Beteiligung verbreiten. Der Datenanbieter hat im Rahmen dieser Prüfung die Daten im Zusammenhang mit der konkreten Kundenfrage auf ihre mögliche Gefährdung der Sicherheitsinteressen hin zu prüfen. Die Prüfung erfolgt anhand von Kriterien, die ihm von der Behörde vorgegeben sind und die eine schnelle, automatisierte Prüfung erlauben. Maßgebliche Kriterien sind dabei der durch Wahl des Sensorbetriebsmodus und Prozessierung erzielte Informationsgehalt der Daten, die Person des Anfragenden sowie dessen Kunden, das angefragte Zielgebiet und die gewünschte Zeitnähe. Ist das Ergebnis dieser Prüfung, dass keine Möglichkeit eines Schadenseintritts für die Sicherheitsinteressen besteht, so kann der Datenanbieter die Daten in den Verkehr bringen oder zugänglich machen. Ein Verwaltungsverfahren ist nicht erforderlich. Aufgrund der Übertragung dieses Teils der Prüfung auf den Datenanbieter muss er für diese Tätigkeit zugelassen und bei der Ausführung von der zuständigen Behörde beaufsichtigt werden. Bezogen auf einzelne Geschäftsvorgänge ist er lediglich zur Dokumentation der Prüfung, des Verfahrens und des Ergebnisses verpflichtet.

Ergibt die Prüfung der Anfrage, dass möglicherweise Sicherheitsinteressen betroffen sind, so kann der Datenanbieter die Daten nur vorbehaltlich einer behördlichen Erlaubnis in den Verkehr bringen oder zugänglich machen. Die Behörde prüft die Anfrage und kann sie ohne Veränderung erlauben oder in bestimmten Fällen die Verwendung und Weitergabe von Daten bestimmter Zielgebiete, das Senden von Daten zu bestimmten Bodensegmenten, den zulässigen Sensorbetriebsmodus, die Verarbeitungsqualität der Daten beschränken oder den Zeitraum zwischen angefragtem Beobachtungszeitpunkt und Auslieferung der Daten vergrößern, um sicherheits- und außenpolitische Interessen zu wahren.

C. Alternativen

Keine

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugsaufwand

Dem Bund entstehen durch das Gesetz keine zusätzlichen Kosten.

Soweit von der öffentlichen Hand geförderte Einrichtungen betroffen sind, werden eventuelle Mehrausgaben im jeweiligen Einzelplan aufgefangen.

2. Vollzugsaufwand

Das Gesetz begründet durch die Schaffung neuer Verwaltungsverfahren Vollzugsaufwand für den Bund. Der Vollzugsaufwand für die Genehmigung von Erdfernerkundungssystemen und die Zulassung von Datenanbietern einschließlich der Aufsichtsaufgaben ist gering. Es handelt sich in den nächsten Jahren um eine überschaubare Zahl von Satellitenbetreibern bzw. Datenanbietern.

Die Bezifferung des Vollzugsaufwands zur Erteilung der Erlaubnis zum Verbreiten von Erdfernerkundungsdaten ist im Einzelnen schwierig, da sowohl technisch als auch fachpolitisch Neuland betreten wird. Zudem hängt sie von der Ausgestaltung der Grenzwerte der Sensitivitätsprüfung ab. Nach derzeitigem Stand kann jedoch der zusätzliche Personalbedarf auf insgesamt elf Personen geschätzt werden, wovon acht auf das Bundesamt für Wirtschaft und Ausfuhrkontrolle als zuständiger Behörde, zwei auf das Bundesministerium für Wirtschaft und Technologie und eine Person auf das Bundesamt für Sicherheit

in der Informationstechnik entfallen. Dies hat Ausgaben von jährlich etwa 0,7 Mio. Euro zur Folge. Dieser Personalbedarf soll soweit wie möglich durch Überhangpersonal aus der Bundesverwaltung gedeckt werden. Eine Überprüfung des Personalaufwands ist nach einer Anlaufphase von zwei Jahren vorgesehen.

E. Sonstige Kosten

Für die betroffenen Unternehmen und Einrichtungen wird zusätzlicher geringfügiger Aufwand durch die Antragserfordernisse sowie durch die einzuführenden Sicherheitsverfahren entstehen. Geringfügige kosteninduzierte Einzelpreisanpassungen lassen sich nicht ausschließen. Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere Verbraucherpreisniveau, sind aber nicht zu erwarten.

F. Bürokratiekosten

Das Gesetz führt Informationspflichten für die betroffenen Betreiber- und Datenanbieterunternehmen ein. Die Zahl der betroffenen Unternehmen dürfte sich in den nächsten Jahren eher im einstelligen Bereich halten. Da mit den beabsichtigten Regelungen sowohl technisch als auch fachpolitisch Neuland betreten wird, ist eine Kostenabschätzung derzeit nicht möglich.

Für die Bürgerinnen und Bürger sowie die Verwaltung werden keine Informationspflichten eingeführt.

Die Ressortabstimmung wurde vor dem 1. Dezember 2006 eingeleitet.



BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

An den
Präsidenten des
Deutschen Bundestages
Herrn Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Berlin, 21. März 2007

Sehr geehrter Herr Präsident,

hiermit übersende ich den von der Bundesregierung beschlossenen

> Entwurf eines Gesetzes zum Schutz vor Gefährdungen der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz – SatDSiG)

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium für Wirtschaft und Technologie.

Der Bundesrat hat in seiner 831. Sitzung am 9. März 2007 gemäß Artikel 76 Absatz 2 des Grundgesetzes beschlossen, zu dem Gesetzentwurf wie aus Anlage 2 ersichtlich Stellung zu nehmen.

Die Auffassung der Bundesregierung zu der Stellungnahme des Bundesrates ist in der als Anlage 3 beigefügten Gegenäußerung dargelegt.

Mit freundlichen Grüßen

Angela Merkel

Anlage 1

Entwurf eines Gesetzes zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz – SatDSiG)

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Teil 1
Anwendungsbereich

§ 1
Anwendungsbereich

(1) Dieses Gesetz gilt

1. für den Betrieb von hochwertigen Erdfernerkundungssystemen
   a) durch deutsche Staatsangehörige, juristische Personen oder Personenvereinigungen deutschen Rechts,
   b) durch ausländische juristische Personen oder Personenvereinigungen, die ihren Verwaltungssitz im Bundesgebiet haben, oder
   c) soweit das unveränderbare Absetzen der Befehlsfolgen zur Kommandierung des Orbitalsystems vom Bundesgebiet aus erfolgt;
2. für den Umgang mit den Daten, die von einem hochwertigen Erdfernerkundungssystem nach Nummer 1 erzeugt worden sind, bis zu deren Verbreiten
   a) durch deutsche Staatsangehörige, juristische Personen oder Personenvereinigungen deutschen Rechts,
   b) durch ausländische juristische Personen oder Personenvereinigungen, die ihren Verwaltungssitz im Bundesgebiet haben, oder
   c) soweit das Verbreiten der Daten vom Bundesgebiet aus erfolgt.

(2) Dieses Gesetz gilt nicht für den Betrieb hochwertiger Erdfernerkundungssysteme durch eine staatliche Stelle mit

militärischen oder nachrichtendienstlichen Aufgaben, soweit die Kenntnisnahme der erzeugten Daten durch Unbefugte ausgeschlossen ist. Von der Anwendung des Gesetzes ist abzusehen, wenn der Betrieb eines hochwertigen Erdfernerkundungssystems nach den Rechtsvorschriften eines anderen Mitgliedstaates der Europäischen Union erlaubt ist und diese Rechtsvorschriften den Regelungen und Schutzinteressen dieses Gesetzes vergleichbar sind. Die zuständige Behörde kann von der Anwendung des Gesetzes absehen, soweit die Rechtsvorschriften eines Drittstaates die Voraussetzungen des Satzes 2 erfüllen und eine völkerrechtliche Vereinbarung zwischen dem Drittstaat und der Bundesrepublik Deutschland besteht, in der die Vergleichbarkeit der Regelungen und Schutzinteressen festgestellt ist.

§ 2
Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes

1. ist Betreiber:

   wer das Erdfernerkundungssystem in eigener Verantwortung steuert;

2. sind Daten:

   Signale eines Sensors oder mehrerer Sensoren eines Orbital- oder Transportsystems und alle daraus abgeleiteten Produkte, unabhängig vom Grad ihrer Verarbeitung und der Art ihrer Speicherung oder Darstellung; Datum im Sinne des § 27 ist jede Einzelangabe;

3. ist Datenanbieter:

   wer Daten, die von einem hochwertigen Erdfernerkundungssystem erzeugt worden sind, verbreitet;

4. ist ein hochwertiges Erdfernerkundungssystem:

   ein raumgestütztes Orbital- oder Transportsystem, einschließlich des Bodensegments, mit dem Daten über die Erde erzeugt werden, soweit dessen Sensor oder Sensoren selbst oder in Kombination mit einem oder mehreren anderen Sensoren technisch in der Lage ist, Daten mit besonders hohem Informationsgehalt im Sinne von Absatz 2 zu erzeugen;

5. ist ein Sensor:

   ein Teil eines raumgestützten Erdfernerkundungssystems, das elektromagnetische Wellen aller Spektralbereiche oder gravimetrische Felder aufzeichnet;

6. ist Verbreiten:

   das Inverkehrbringen oder das Zugänglichmachen der Daten für Dritte.

(2) Das Bundesministerium für Wirtschaft und Technologie hat durch Rechtsverordnung ohne Zustimmung des Bundesrates Bestimmungen zu erlassen, unter welchen Voraussetzungen Daten einen besonders hohen Informationsgehalt haben. Der Informationsgehalt ist dabei zu bestimmen nach

1. der geometrischen Auflösung,
2. der spektralen Abdeckung,
3. der Zahl der Spektralkanäle und der spektralen Auflösung,
4. der radiometrischen Auflösung und
5. der zeitlichen Auflösung.

Bei Mikrowellen- oder Radarsensoren ist der Informationsgehalt auch zu bestimmen nach

1. den Polarisationsmerkmalen und
2. der Phasengeschichte.

Die Bestimmungen berücksichtigen die möglichen Auswirkungen, die ein Verbreiten von Daten mit besonders hohem Informationsgehalt auf die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker und die auswärtigen Beziehungen der Bundesrepublik Deutschland hat.

Teil 2
Betrieb eines hochwertigen Erdfernerkundungssystems

§ 3
Genehmigung

(1) Der Betrieb eines hochwertigen Erdfernerkundungssystems bedarf der Genehmigung.

(2) Nachträgliche Änderungen der Genehmigung sind zulässig, wenn dies erforderlich ist, um die Einhaltung der Genehmigungsvoraussetzungen im Falle nachträglich eingetretener Tatsachen oder einer geänderten Rechtsvorschrift sicherzustellen.

(3) Anforderungen anderer Gesetze an den Betrieb eines hochwertigen Erdfernerkundungssystems bleiben unberührt. Die Genehmigung wird unbeschadet privater Rechte Dritter erteilt.

(4) Ist ein raumgestütztes Erdfernerkundungssystem nicht hochwertig, so hat die zuständige Behörde dies auf Antrag des Betreibers festzustellen. Entfällt nachträglich das Genehmigungserfordernis durch Änderung der Bestimmungen nach § 2 Abs. 2, so erlischt die Genehmigung.

§ 4
Genehmigungsvoraussetzungen

(1) Die Genehmigung ist zu erteilen, wenn

1. der Betreiber des hochwertigen Erdfernerkundungssystems die erforderliche Zuverlässigkeit besitzt,
2. die Befehlsfolgen zur
   a) Kommandierung des Orbital- oder Transportsystems,
   b) Steuerung des Sensors oder der Sensoren,
   c) Steuerung der Übermittlung der Daten durch das Orbital- oder Transportsystem an ein Bodensegment des Betreibers oder einer nach § 11 zugelassenen Person und
   d) Steuerung des Verbreitens der Daten unmittelbar durch das Orbital- oder Transportsystem

   im Bundesgebiet hergestellt und durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen Veränderung durch Dritte geschützt werden,
3. die Übermittlung der Daten durch das Orbital- oder Transportsystem an ein Bodensegment des Betreibers oder einer nach § 11 zugelassenen Person, die Übermittlung der Daten zwischen verschiedenen Standorten des Bodensegments des Betreibers und die Übermittlung der Daten vom Betreiber an eine nach § 11 zugelassene Per-

son durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen unbefugte Kenntnisnahme geschützt sind, und

4. der Betreiber technische und organisatorische Maßnahmen getroffen hat, die verhindern, dass Unbefugte Zugang zu den Anlagen der Kommandierung des hochwertigen Erdfernerkundungssystems sowie zu den Anlagen zum Empfang, zur Verarbeitung und zur Speicherung der Daten oder Zutritt zu den dafür genutzten Betriebsräumen haben.

(2) Der Betreiber hat Personen, welche Zugang zu den Anlagen der Kommandierung eines hochwertigen Erdfernerkundungssystems oder zu den Anlagen zum Empfang, zur Verarbeitung und zur Speicherung der Daten solcher Systeme haben, durch die zuständige Behörde einer einfachen Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz unterziehen zu lassen.

§ 5
Dokumentationspflicht

(1) Der Betreiber eines hochwertigen Erdfernerkundungssystems ist verpflichtet,

1. die Befehlsfolgen zur Kommandierung des Orbital- oder Transportsystems,
2. die Befehlsfolgen zur Steuerung des Sensors oder der Sensoren,
3. Angaben zu Verschlüsselungsverfahren, verwendeten Schlüsseln und Schlüsselmanagement und
4. den Zeitpunkt und den Weg der Befehlsfolgen

aufzuzeichnen.

(2) Die Aufzeichnungen nach Absatz 1 sind mindestens fünf Jahre nach Ausführung der jeweiligen Befehlsfolge aufzubewahren und zur Einsichtnahme durch die zuständige Behörde bereitzuhalten.

§ 6
Anzeigepflicht

(1) Der Betreiber eines hochwertigen Erdfernerkundungssystems hat der zuständigen Behörde

1. Änderungen von Tatsachen, die er zur Eintragung in das Handels- oder Vereinsregister anzumelden hat, und
   a) soweit der Betreiber in der Rechtsform einer Personenhandelsgesellschaft tätig ist, Änderungen des Gesellschaftsvertrages oder
   b) soweit der Betreiber in der Rechtsform einer Gesellschaft mit beschränkter Haftung tätig ist, Änderungen in den Personen der Gesellschafter oder des Umfangs ihrer Beteiligung,
2. tatsächliche Anhaltspunkte dafür, dass ein Dritter die Befehlsfolgen zur Kommandierung des Orbital- oder Transportsystems, zur Steuerung des Sensors oder der Sensoren oder zur Steuerung der Übermittlung der Daten vom Orbital- oder Transportsystem absetzt oder abzusetzen versucht, sowie
3. Änderungen der nach § 4 Abs. 1 Nr. 4 getroffenen Maßnahmen

unverzüglich schriftlich anzuzeigen.

(2) Der Betreiber eines hochwertigen Erdfernerkundungssystems hat der zuständigen Behörde unverzüglich schriftlich anzuzeigen, an welche nach § 11 zugelassenen Personen er Daten übermittelt.

§ 7
Auskunftspflicht

(1) Der Betreiber eines hochwertigen Erdfernerkundungssystems hat der zuständigen Behörde auf Verlangen Auskünfte zu erteilen und Unterlagen vorzulegen, soweit dies zur Überwachung der Einhaltung dieses Gesetzes und der zu diesem Gesetz erlassenen Rechtsverordnungen erforderlich ist.

(2) Auskunftspflichtige Personen können die Auskunft auf solche Fragen verweigern, deren Beantwortung sie selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr einer strafrechtlichen Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

§ 8
Betretens- und Prüfungsrechte

Die Beauftragten der zuständigen Behörde sind befugt, zu den üblichen Betriebs- und Geschäftszeiten die Betriebs- und Geschäftsräume des Betreibers eines hochwertigen Erdfernerkundungssystems zu betreten und die zur Erfüllung ihrer Aufgaben erforderlichen Prüfungen vorzunehmen; die §§ 196, 197 Abs. 1 Satz 1 und 2 und Abs. 2, §§ 198, 199 Abs. 2 und §§ 200 bis 202 der Abgabenordnung gelten entsprechend.

§ 9
Maßnahmen der zuständigen Behörde

(1) Die zuständige Behörde kann gegenüber dem Betreiber eines hochwertigen Erdfernerkundungssystems im Einzelfall diejenigen Maßnahmen anordnen, die zur ordnungsgemäßen Erfüllung seiner Pflichten erforderlich sind.

(2) Die zuständige Behörde kann insbesondere

1. vorübergehend die Übermittlung von Daten an ein Bodensegment oder an eine nach § 11 zugelassene Person untersagen oder
2. anordnen, den Betrieb ganz oder teilweise auf einen geeigneten Sonderbeauftragten zu übertragen.

(3) Die durch die Bestellung des Sonderbeauftragten entstehenden Kosten einschließlich der diesem zu gewährenden Vergütung trägt der Betreiber des hochwertigen Erdfernerkundungssystems. Die zuständige Behörde setzt die Höhe der Vergütung fest.

§ 10
Erwerb von Unternehmen und Unternehmensbeteiligungen; Betriebsübernahme

(1) Der Erwerb eines Unternehmens, das ein hochwertiges Erdfernerkundungssystem betreibt, oder der Erwerb einer unmittelbaren oder mittelbaren Beteiligung an einem solchen Unternehmen durch

1. ausländische Staatsangehörige, juristische Personen oder Personenvereinigungen ausländischen Rechts oder

2. juristische Personen oder Personenvereinigungen deutschen Rechts, an denen ausländische Staatsangehörige, juristische Personen oder Personenvereinigungen ausländischen Rechts mindestens 25 Prozent der Stimmrechte halten,

ist vom Erwerber der zuständigen Behörde unverzüglich zu melden. Dies gilt nicht, wenn der unmittelbare oder mittelbare Stimmrechtsanteil des Erwerbers an dem betreffenden Unternehmen nach dem Erwerb der Beteiligung 25 Prozent nicht erreicht. Bei der Berechnung des Stimmrechtsanteils des Erwerbers sind diesem die Anteile anderer Unternehmen an dem zu erwerbenden Unternehmen zuzurechnen, wenn der Erwerber mindestens 25 Prozent oder mehr der Stimmrechte an dem anderen Unternehmen hält. Die zuständige Behörde kann den Erwerb innerhalb eines Monats nach Eingang der vollständigen Unterlagen über den Erwerb untersagen, soweit dies erforderlich ist, um die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland zu gewährleisten.

(2) Die vollständige oder teilweise Übernahme des Betriebs eines hochwertigen Erdfernerkundungssystems oder von Teilen eines solchen bedarf der Erlaubnis, wenn durch die Übernahme die Genehmigungspflicht nach § 3 Abs. 1 entfällt. Der Antrag auf Erteilung der Erlaubnis ist vom Übernehmenden zu stellen. Die Erlaubnis ist zu erteilen, wenn der weitere Betrieb des hochwertigen Erdfernerkundungssystems oder von Teilen des hochwertigen Erdfernerkundungssystems die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland nicht gefährdet.

Teil 3
Verbreiten von Daten

Kapitel 1
Allgemeine Voraussetzungen

§ 11
Zulassung

(1) Ein Datenanbieter, der Daten verbreiten will, bedarf der Zulassung.

(2) Nachträgliche Änderungen der Zulassung sind zulässig, wenn dies erforderlich ist, um die Einhaltung der Zulassungsvoraussetzungen im Falle nachträglich eingetretener Tatsachen oder einer geänderten Rechtsvorschrift sicherzustellen.

§ 12
Zulassungsvoraussetzungen

(1) Die Zulassung ist zu erteilen, wenn

1. der Datenanbieter die erforderliche Zuverlässigkeit besitzt,
2. der Datenanbieter technische und organisatorische Maßnahmen getroffen hat, die verhindern, dass Unbefugte Zugang zu den Anlagen zum Empfang, zur Verarbeitung und zur Speicherung von Daten eines hochwertigen Erdfernerkundungssystems oder Zutritt zu den dafür genutzten Betriebsräumen haben,
3. die Übermittlung der Daten zwischen verschiedenen Standorten des Bodensegments des Datenanbieters und die Übermittlung der Daten an einen anderen Datenanbieter durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen unbefugte Kenntnisnahme geschützt sind und
4. das sichere Verbreiten der von einem hochwertigen Erdfernerkundungssystem erzeugten Daten nach dem Stand der Technik gewährleistet ist.

(2) Der Datenanbieter hat Personen, welche Zugang zu den Anlagen zum Empfang, zur Verarbeitung und zur Speicherung von Daten eines hochwertigen Erdfernerkundungssystems haben, durch die zuständige Behörde einer einfachen Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz unterziehen zu lassen.

§ 13
Anzeigepflicht

Der Datenanbieter hat der zuständigen Behörde

1. Änderungen von Tatsachen, die er zur Eintragung in das Handels- oder Vereinsregister anzumelden hat, und
   a) soweit der Datenanbieter in der Rechtsform einer Personenhandelsgesellschaft tätig ist, Änderungen des Gesellschaftsvertrages oder
   b) soweit der Datenanbieter in der Rechtsform einer Gesellschaft mit beschränkter Haftung tätig ist, Änderungen in den Personen der Gesellschafter oder des Umfangs ihrer Beteiligung,
2. Änderungen der nach § 12 Abs. 1 Nr. 2 getroffenen Maßnahmen sowie
3. tatsächliche Anhaltspunkte dafür, dass die Sicherung der Daten, die mit einem hochwertigen Erdfernerkundungssystem erzeugt worden sind, nicht aufrechterhalten wird,

unverzüglich schriftlich anzuzeigen.

§ 14
Auskunftspflicht

(1) Der Datenanbieter hat der zuständigen Behörde auf Verlangen Auskünfte zu erteilen und Unterlagen vorzulegen, soweit dies zur Überwachung der Einhaltung dieses Gesetzes und der zu diesem Gesetz erlassenen Rechtsverordnungen erforderlich ist.

(2) Der Datenanbieter kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr einer strafrechtlichen Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

§ 15
Betretens- und Prüfungsrechte

Die Beauftragten der zuständigen Behörde sind befugt, zu den üblichen Betriebs- und Geschäftszeiten die Betriebs- und Geschäftsräume des Datenanbieters zu betreten und die zur Erfüllung ihrer Aufgaben erforderlichen Prüfungen durchzuführen; die §§ 196, 197 Abs. 1 Satz 1 und 2 und Abs. 2, §§ 198, 199 Abs. 2 und §§ 200 bis 202 der Abgabenordnung gelten entsprechend.

§ 16
Maßnahmen der zuständigen Behörde

Die zuständige Behörde kann gegenüber dem Datenanbieter im Einzelfall diejenigen Maßnahmen anordnen, die zur ordnungsgemäßen Erfüllung seiner Pflichten erforderlich sind. Sie kann insbesondere

1. verlangen, das Verbreiten der Daten dem Stand der Technik anzupassen, oder
2. vorübergehend das Verbreiten von Daten untersagen.

Kapitel 2
Verfahren des Verbreitens von Daten

§ 17
Sensitivitätsprüfung

(1) Der Datenanbieter, der eine Anfrage auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems bedienen will, hat die Anfrage nach Maßgabe einer Rechtsverordnung nach Absatz 3 auf ihre Sensitivität zu prüfen.

(2) Eine Anfrage ist sensitiv, wenn

1. der durch den verwendeten Sensorbetriebsmodus und durch die verwendete Verarbeitung erzielte Informationsgehalt der Daten,
2. das mit den Daten dargestellte Zielgebiet,
3. der Zeitpunkt der Erzeugung der Daten und der Zeitraum zwischen der Erzeugung der Daten und der Bedienung der Anfrage und
4. die Bodensegmente, an welche die Daten übermittelt werden sollen,

in ihrer Zusammenschau die Möglichkeit eines Schadenseintritts für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker oder die auswärtigen Beziehungen der Bundesrepublik Deutschland ergeben. Die Zusammenschau nach Satz 1 erfolgt in Ansehung der Person des Anfragenden und soll die Personen berücksichtigen, die bestimmungsgemäß mit den Daten in Kontakt kommen, einschließlich deren gewöhnlichen Aufenthaltsortes. Der Datenanbieter hat dazu die Identität des Anfragenden in geeigneter Weise zu prüfen und die Nennung der Personen einschließlich deren gewöhnlichen Aufenthaltsortes zu verlangen, die bestimmungsgemäß mit den Daten in Kontakt kommen.

(3) Das Bundesministerium für Wirtschaft und Technologie hat im Einvernehmen mit dem Bundesministerium der Verteidigung, dem Auswärtigen Amt und dem Bundesministerium des Innern durch Rechtsverordnung ohne Zustimmung des Bundesrates Bestimmungen zu erlassen, unter welchen Voraussetzungen nach Absatz 2 die Möglichkeit eines Schadenseintritts für die genannten Schutzgüter gegeben ist. Dabei berücksichtigt es regelmäßig zu aktualisierende Feststellungen der Sicherheitsanforderungen der betroffenen Behörden, die Verpflichtungen und Vereinbarungen der Bundesrepublik Deutschland gegenüber den Mitgliedstaaten der Europäischen Union, den Parteien des Nordatlantikvertrages vom 4. April 1949 (BGBl. 1955 II S. 289) in der Fassung des Protokolls vom 17. Oktober 1951 (BGBl. 1955 II S. 293) und gegenüber Australien, Japan, Neuseeland und der Schweiz, den Stand der Technik in Bezug auf die Erzeugung von Daten mit besonders hohem Informationsgehalt, die bestehenden Regelungen, unter denen der Anfragende die Daten weiter übermitteln könnte, und die Verfügbarkeit von vergleichbaren Daten auf internationalen Märkten. In der Rechtsverordnung ist festzulegen, nach welchem Verfahren die Zusammenschau nach Absatz 2 Satz 1 und 2 erfolgt. Die Rechtsverordnung darf dem Datenanbieter keinen eigenen Einschätzungsspielraum belassen, ob eine Anfrage sensitiv ist. Auf bevorstehende Änderungen der Rechtsverordnung kann der Datenanbieter hingewiesen werden. Das Bundesministerium für Wirtschaft und Technologie kann im Einvernehmen mit dem Bundesministerium der Verteidigung und dem Auswärtigen Amt die Ermächtigung durch Rechtsverordnung ohne Zustimmung des Bundesrates ganz oder teilweise auf das Bundesamt für Wirtschaft und Ausfuhrkontrolle übertragen.

§ 18
Dokumentationspflicht

(1) Der Datenanbieter ist verpflichtet, alle Anfragen auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems aufzuzeichnen. Dies umfasst

1. die Anfrage einschließlich der Personen, die bestimmungsgemäß mit den Daten in Kontakt kommen, und deren gewöhnlichen Aufenthaltsortes,
2. die Prüfung der Identität des Anfragenden,
3. das Verfahren und das Ergebnis der Prüfung auf Sensitivität der Anfrage nach § 17 Abs. 1 in Verbindung mit den Bestimmungen einer Rechtsverordnung nach § 17 Abs. 3,
4. den Auftrag gegenüber dem Betreiber des hochwertigen Erdfernerkundungssystems auf Erzeugung der Daten,
5. die Empfangsprotokolle von Bodensegmenten,
6. die Angaben zu Verschlüsselungsverfahren, verwendeten Schlüsseln und Schlüsselmanagement,
7. die Protokolle der Verarbeitungsketten des Bodensegments,
8. die Metadaten der Daten, insbesondere das Zielgebiet, den Zeitpunkt der Erzeugung der Daten, den Sensorbetriebsmodus und die Parameter der Verarbeitung der Daten,
9. die Transferprotokolle oder Lieferscheine einschließlich Auslieferungsbestätigungen in Bezug auf die Bedienung der Anfrage und
10. die Rechnungen.

Die Sätze 1 und 2 Nr. 4 bis 10 gelten entsprechend, wenn Daten ohne Anfrage verbreitet werden. Wird eine Anfrage auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems aus einem Archiv ausgeführt, so ist für die Protokollierung und Dokumentation nach Satz 2 Nr. 4 und 5 ein Verweis auf eine anderweitige Protokollierung und Dokumentation ausreichend.

(2) Die Aufzeichnungen nach Absatz 1 sind mindestens fünf Jahre nach Entstehung der jeweiligen Daten aufzubewahren und zur Einsichtnahme durch die zuständige Behörde bereitzuhalten.

(3) Der Datenanbieter ist verpflichtet, gleichartige Protokolle und Dokumentationen fremder Bodensegmente bereitzuhalten, die er bei der Bedienung der Anfrage auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems einsetzt. Absatz 2 gilt entsprechend.

(4) Der Datenanbieter hat dem Anfragenden die Aufbewahrung der Daten und die Möglichkeit der behördlichen Einsichtnahme mitzuteilen.

§ 19
Erlaubnis

(1) Will ein Datenanbieter eine sensitive Anfrage bedienen, bedarf er der Erlaubnis. Dies gilt auch, wenn er Daten eines hochwertigen Erdfernerkundungssystems ohne Anfrage verbreiten will.

(2) Die Erlaubnis nach Absatz 1 ist zu erteilen, wenn das Verbreiten der Daten im Einzelfall die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland nicht gefährdet, das friedliche Zusammenleben der Völker nicht und die auswärtigen Beziehungen der Bundesrepublik Deutschland nicht erheblich stört.

(3) Die zuständige Behörde soll über den Antrag auf Erlaubnis spätestens einen Monat nach Eingang entscheiden.

(4) Die Erlaubnis wird unbeschadet privater Rechte Dritter erteilt.

§ 20
Sammelerlaubnis

Die zuständige Behörde kann eine Sammelerlaubnis erteilen, wenn ein Datenanbieter

1. Darstellungen von Daten mit stark vermindertem Informationsgehalt oder Metadaten für jedermann zugänglich machen oder
2. sensitive Anfragen, die in gleichartiger Weise von derselben Person für eine unbestimmte Anzahl von Daten eines hochwertigen Erdfernerkundungssystems angefragt werden, bedienen will.

Die Sammelerlaubnis ergeht unter den Voraussetzungen des § 19 Abs. 2 und darf nur unter Vorbehalt des Widerrufs erteilt werden. Eine Sammelerlaubnis nach Satz 1 Nr. 1 hat zu bestimmen, welchen Informationsgehalt die Daten höchstens haben dürfen. Eine Sammelerlaubnis nach Satz 1 Nr. 2 darf nur für eine bestimmte Frist erteilt werden, die drei Jahre nicht überschreiten soll.

Teil 4
Vorrangige Bedienung von Anfragen der Bundesrepublik Deutschland

§ 21
Verpflichtung des Datenanbieters

In folgenden Fällen ist der Datenanbieter verpflichtet, Anfragen der Bundesrepublik Deutschland, vertreten durch das Bundeskanzleramt, auf Verbreiten von Daten gegenüber jeder anderen Anfrage vorrangig zu bedienen:

1. im Bündnisfall gemäß Artikel 5 des Nordatlantikvertrages vom 4. April 1949 (BGBl. 1955 II S. 289) in der Fassung des Protokolls vom 17. Oktober 1951 (BGBl. 1955 II S. 293),
2. im Verteidigungsfall gemäß Artikel 115 Buchstabe a bis l des Grundgesetzes,
3. wenn die Voraussetzung des inneren Notstandes gemäß Artikel 91 des Grundgesetzes vorliegen,
4. im Spannungsfall gemäß Artikel 80a des Grundgesetzes oder
5. wenn im Ausland eingesetzte militärische oder zivile Kräfte der Bundesrepublik Deutschland oder an den deutschen Auslandsvertretungen tätige Beschäftigte des auswärtigen Dienstes, die einer konkreten Beeinträchtigung der äußeren Sicherheit der Bundesrepublik Deutschland entgegenwirken, gegenwärtig gefährdet sind.

§ 22
Verpflichtung des Betreibers

Der Betreiber eines hochwertigen Erdfernerkundungssystems ist verpflichtet, in den Fällen des § 21 Aufträge zur Erzeugung von Daten für die Bundesrepublik Deutschland gegenüber jedem anderen Auftrag zur Erzeugung von Daten vorrangig zu behandeln. Unbeschadet des Satzes 1 soll die Erdfernerkundungsanfrage der Bundesrepublik Deutschland, vertreten durch das Bundeskanzleramt, bei einem Datenanbieter erfolgen. Erfolgt diese dennoch bei dem Betreiber eines hochwertigen Erdfernerkundungssystems, bedarf dieser zum Verbreiten dieser Daten keiner Zulassung nach § 11.

§ 23
Vergütung

(1) Unbeschadet der Verpflichtungen aus diesem Teil kann für die Erzeugung der Daten nach § 22 sowie für die Bedienung der Anfrage nach § 21 eine Vergütung verlangt werden. Die Vergütung soll dem jeweiligen durchschnittlichen Marktpreis entsprechen.

(2) Weitergehende Ansprüche gegen die Bundesrepublik Deutschland sind ausgeschlossen.

Teil 5
Durchführungsvorschriften

§ 24
Zuständigkeit

(1) Zuständige Behörde nach diesem Gesetz ist vorbehaltlich der Absätze 2 und 3 das Bundesamt für Wirtschaft und Ausfuhrkontrolle.

(2) Zuständig für die Durchführung einer Sicherheitsüberprüfung nach § 4 Abs. 2 und § 12 Abs. 2 ist das Bundesministerium für Wirtschaft und Technologie.

(3) Eine Meldung nach § 10 Abs. 1 Satz 1 erfolgt an das Bundesministerium für Wirtschaft und Technologie. Das Bundesministerium für Wirtschaft und Technologie ist im Einvernehmen mit dem Auswärtigen Amt und dem Bundesministerium der Verteidigung zuständig für eine Untersagung des Erwerbs von Unternehmen oder Unternehmensbeteiligungen nach § 10 Abs. 1 Satz 3.

§ 25
Verfahren

(1) Eine Genehmigung nach § 3 Abs. 1, eine Zulassung nach § 11 Abs. 1 und eine Erlaubnis nach § 10 Abs. 2 Satz 1, § 19 Abs. 1 Satz 1 und 2 sowie nach § 20 Satz 1 setzen je-

weils einen schriftlichen Antrag voraus. Eine Meldung nach § 10 Abs. 1 Satz 1 hat schriftlich zu erfolgen. Einem Antrag oder einer Meldung sind die zur Prüfung der Erteilungsvoraussetzungen notwendigen Unterlagen beizufügen.

(2) Zur Feststellung der Eignung eines Verfahrens nach § 4 Abs. 1 Nr. 2 und 3 ist das Bundesamt für Sicherheit in der Informationstechnik frühzeitig zu beteiligen. Das Bundesamt für Sicherheit in der Informationstechnik stellt dem Antragsteller Unterlagen zum Umfang und Ablauf der Prüfung zur Verfügung.

(3) Verwaltungsakte nach diesem Gesetz sind schriftlich zu erlassen und zuzustellen.

§ 26
Gebühren und Auslagen

Für Amtshandlungen nach diesem Gesetz erhebt die zuständige Behörde Gebühren und Auslagen. Das Bundesministerium für Wirtschaft und Technologie wird ermächtigt, die Gebührentatbestände, die Gebührenhöhe und die zu erstattenden Auslagen durch Rechtsverordnung ohne Zustimmung des Bundesrates zu bestimmen und dabei feste Sätze oder Rahmensätze vorzusehen. Die Gebührensätze sind so zu bemessen, dass die mit den Amtshandlungen verbundenen Kosten gedeckt sind. Die Bedeutung, der wirtschaftliche Wert oder sonstige Nutzen der Amtshandlung für den Begünstigten werden angemessen berücksichtigt.

§ 27
Übermittlung von personenbezogenen Daten, Betriebs- und Geschäftsgeheimnissen

(1) Die zuständige Behörde kann personenbezogene Daten, die ihr bei der Erfüllung ihrer Aufgaben nach diesem Gesetz bekannt geworden sind, an andere Behörden übermitteln, soweit die Kenntnis der personenbezogenen Daten aus ihrer Sicht erforderlich ist

1. zur Abwehr einer Gefahr für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland oder zur Verhinderung einer Störung des friedlichen Zusammenlebens der Völker oder einer erheblichen Störung der auswärtigen Beziehungen der Bundesrepublik Deutschland oder
2. zur Verhütung oder zur Verfolgung von Straftaten.

Eine Übermittlung nach Satz 1 Nr. 2 ist nur zulässig, wenn tatsächliche Anhaltspunkte für die zukünftige Begehung oder das Vorliegen von Straftaten bestehen. Darüber hinaus kann die zuständige Behörde diese personenbezogenen Daten an den Bundesnachrichtendienst übermitteln, wenn die Voraussetzungen des § 8 Abs. 3 des BND-Gesetzes erfüllt sind. Der Dritte, an den die personenbezogenen Daten übermittelt werden, darf diese nur für den Zweck verwenden, zu dessen Erfüllung sie übermittelt werden.

(2) In Strafverfahren wegen eines Verstoßes gegen dieses Gesetz dürfen Gerichte und Staatsanwaltschaften obersten Bundesbehörden personenbezogene Daten übermitteln, wenn dies zur Abwehr einer Gefahr für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland oder zur Verhinderung einer Störung des friedlichen Zusammenlebens der Völker oder einer erheblichen Störung der auswärtigen Beziehungen der Bundesrepublik Deutschland erforderlich ist. Die nach Satz 1 erlangten personenbezogenen Daten dürfen nur zu den dort genannten Zwecken verwendet werden. Der Dritte, an den die personenbezogenen Daten übermittelt werden, darf diese an eine nicht in Satz 1 genannte öffentliche Stelle zudem nur weiter übermitteln, wenn das Interesse an der Verwendung der übermittelten personenbezogenen Daten das Interesse des Betroffenen an der Geheimhaltung erheblich überwiegt und der Untersuchungszweck des Strafverfahrens nicht gefährdet werden kann.

(3) Betriebs- und Geschäftsgeheimnisse stehen personenbezogenen Daten gleich.

Teil 6
Bußgeldvorschriften, Strafvorschriften

§ 28
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. ohne Genehmigung nach § 3 Abs. 1 ein hochwertiges Erdfernerkundungssystem betreibt,
2. entgegen § 10 Abs. 1 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erstattet oder einer vollziehbaren Anordnung nach § 10 Abs. 1 Satz 4 zuwiderhandelt,
3. ohne Erlaubnis
   a) nach § 10 Abs. 2 Satz 1 den Betrieb eines hochwertigen Erdfernerkundungssystems oder von Teilen eines solchen übernimmt,
   b) nach § 19 Abs. 1 Satz 1 eine sensitive Anfrage bedient oder
   c) nach § 19 Abs. 1 Satz 2 Daten ohne Anfrage verbreitet,
4. einer vollziehbaren Anordnung nach § 9 Abs. 1, 2 oder § 16 zuwiderhandelt,
5. ohne Zulassung nach § 11 Abs. 1 Daten verbreitet,
6. entgegen § 17 Abs. 1 in Verbindung mit den Bestimmungen einer Rechtsverordnung nach § 17 Abs. 3 eine Anfrage auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems nicht, nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise auf dessen Sensitivität prüft,
7. entgegen § 5 Abs. 1 oder § 18 Abs. 1 Satz 1 und 2 eine Aufzeichnung nicht, nicht richtig oder nicht vollständig fertigt oder diese Aufzeichnungen nach § 5 Abs. 2 oder § 18 Abs. 2 nicht oder nicht mindestens fünf Jahre aufbewahrt oder
8. entgegen § 18 Abs. 3 Satz 1 keine dort genannten Protokolle und Dokumentationen bereithält.

(2) Ordnungswidrig handelt, wer

1. entgegen § 6 Abs. 1 oder § 13 eine Anzeige nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erstattet oder
2. entgegen § 7 Abs. 1 oder § 14 Abs. 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt.

(3) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nr. 1 bis 5 mit einer Geldbuße bis zu fünfhunderttausend Euro, in den Fällen des Absatzes 1 Nr. 6 bis 8 mit einer Geldbuße bis zu fünfzigtausend Euro und in den Fällen des Absatzes 2 mit einer Geldbuße von bis zu fünfundzwanzigtausend Euro geahndet werden.

§ 29
Straftaten

(1) Mit Freiheitsstrafe bis fünf Jahren oder mit Geldstrafe wird bestraft, wer eine in § 28 Abs. 1 Nr. 1 bis 6 bezeichnete vorsätzliche Handlung begeht, die geeignet ist,

1. die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland,
2. das friedliche Zusammenleben der Völker oder
3. die auswärtigen Beziehungen der Bundesrepublik Deutschland erheblich

zu gefährden.

(2) Der Versuch ist strafbar.

§ 30
Auslandstaten Deutscher

§ 29 gilt, unabhängig vom Recht des Tatorts, auch im Ausland, wenn der Täter zur Zeit der Tat Deutscher ist.

§ 31
Straf- und Bußgeldverfahren

(1) Soweit für Straftaten nach § 29 das Amtsgericht sachlich zuständig ist, ist örtlich zuständig das Amtsgericht, in dessen Bezirk das Landgericht seinen Sitz hat.

(2) Im Strafverfahren gelten § 49 Abs. 2, § 63 Abs. 2 und 3 Satz 1 sowie § 76 Abs. 1 und 4 des Gesetzes über Ordnungswidrigkeiten über die Beteiligung der Verwaltungsbehörden im Verfahren der Staatsanwaltschaft und im gerichtlichen Verfahren entsprechend.

Teil 7
Übergangs- und Schlussbestimmungen

§ 32
Änderung des Bundesverfassungsschutzgesetzes

§ 3 Abs. 2 des Bundesverfassungsschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 2 des Gesetzes vom 21. Juni 2005 (BGBl. I S. 1818) geändert worden ist, wird wie folgt geändert:

1. In Satz 1 werden nach Nummer 3 der Punkt durch ein Komma ersetzt und folgende Nummer 4 angefügt:

   „4. bei der Überprüfung von Personen in sonstigen gesetzlich bestimmten Fällen.“

2. In Satz 2 wird die Angabe „Nr. 1 und 2“ durch die Angabe „Nr. 1, 2 und 4“ ersetzt.

§ 33
Änderung des Sicherheitsüberprüfungsgesetzes

Das Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867), das zuletzt durch Artikel 7 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407) geändert worden ist, wird wie folgt geändert:

1. In § 1 Abs. 2 werden nach Nummer 3 der Punkt durch ein Komma ersetzt und folgende Nummer 4 angefügt:

   „4. nach anderen Vorschriften einer Sicherheitsüberprüfung unterliegt, soweit auf dieses Gesetz verwiesen wird.“

2. In § 3 Abs. 2 Satz 1 wird die Angabe „nach § 3 Abs. 2 Nr. 1“ durch die Angabe „nach § 3 Abs. 2 Nr. 1, 2 und 4“ ersetzt.

3. In § 24 wird der Satzteil „mit einer sicherheitsempfindlichen Tätigkeit nach § 1 Abs. 4 bei einer nichtöffentlichen Stelle betraut werden sollen“ durch den Satzteil „von einer nichtöffentlichen Stelle mit einer sicherheitsempfindlichen Tätigkeit nach § 1 Abs. 2 Nr. 4 oder Abs. 4 betraut werden sollen“ ersetzt.

§ 34
Übergangsregelung

(1) Der bei Inkrafttreten dieses Gesetzes bestehende Betrieb eines hochwertigen Erdfernerkundungssystems gilt bis zum Eintritt der Unanfechtbarkeit der Entscheidung über den Genehmigungsantrag als genehmigt, wenn dieser Antrag innerhalb von drei Monaten ab Inkrafttreten dieses Gesetzes gestellt wird.

(2) Absatz 1 gilt entsprechend für die Zulassung als Datenanbieter. Die Pflichten des Datenanbieters nach § 17 Abs. 1 und § 19 Abs. 1 gelten bis zum Inkrafttreten der Rechtsverordnung nach § 17 Abs. 3 als erfüllt.

§ 35
Inkrafttreten

(1) § 2 Abs. 2, § 17 Abs. 3 und § 26 Satz 2 bis 4 treten am Tag nach der Verkündung in Kraft.

(2) Im Übrigen tritt dieses Gesetz am 1. Juli 2007 in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit

Ziel des Gesetzes ist die Wahrung sicherheits- und außenpolitischer Interessen der Bundesrepublik Deutschland. Diese Interessen können durch die Weitergabe und Vermarktung von Erdfernerkundungsdaten gefährdet sein.

Die Nutzung von Erdfernerkundungssystemen und das Verbreiten damit erzeugter Daten sind militärisch relevant und sowohl für die innere und äußere Sicherheit der Bundesrepublik Deutschland als auch für die Sicherheit verbündeter wie auch dritter Staaten von Bedeutung. Auch wenn Erdfernerkundungssysteme und Daten, die mit diesen erzeugt werden, keine originäre Sicherheitsgefährdung darstellen, haben Erdfernerkundungsdaten einen erheblichen wirkungsverstärkenden Effekt: Wirkungen von Waffen, militärische Wirkungen oder politische Drohungen können durch Erdfernerkundungsdaten erheblich verstärkt werden. Die Daten, welche in den Anwendungsbereich des Gesetzes fallen, können beispielsweise zur Erstellung von Höhenprofilen, die zur Steuerung und Zielführung von Lenkflugkörpern oder unbemannten Luftfahrzeugen geeignet sind, verwendet werden. Auch besitzen sie das Potenzial militärischer oder terroristischer Zielerkennung und -ortung von hochsensiblen Zielen im In- und Ausland, wie beispielsweise Truppenstützpunkten. Ein unkontrolliertes Verbreiten solcher Daten von Deutschland aus oder mit Erdfernerkundungssystemen deutscher Bauart liefe auch dem Friedensgebot des Artikels 26 des Grundgesetzes (GG) zuwider. Das gilt nicht nur für die Nutzung der Daten in zwischenstaatlichen Konflikten, sondern auch durch nichtstaatliche Akteure bei Gewaltanwendung unterhalb einer kriegerischen Auseinandersetzung, beispielsweise in ethnischen Konflikten, bei bürgerkriegsähnlichen Unruhen oder terroristischen Akten. Politisch kann die Bundesrepublik Deutschland hierdurch auch Vorwürfen ausgesetzt sein, dass militärisch verwendbare Daten von deutschen Erdfernerkundungssystemen infolge fehlender Kontrolle an Dritte gelangen und hierdurch zur Gefährdung für andere Staaten werden. Die Zuverlässigkeit Deutschlands im Umgang mit militärisch verwendbaren Daten könnte hierdurch in Frage gestellt werden.

Um eine solche Gefährdung auszuschließen, bietet das Gesetz die Möglichkeit der Beschränkung des Inverkehrbringens oder Zugänglichmachens solcher Daten. Mit dem Gesetz wird die nationale Datensicherheitspolitik der Bundesregierung umgesetzt.

Ein Gesetz wird erforderlich, weil in Deutschland zurzeit außergewöhnlich leistungsfähige Erdbeobachtungssatelliten mit dem Ziel einer gewerblichen weltweiten Vermarktung der Daten entstehen. Im Besonderen trifft dies auf die Public-Private-Partnership-Projekte „TerraSAR-X“ und „RapidEye“ (beide Start 2007), aber auch auf in der Vorbereitung befindlichen Projekte wie „TanDEM-X“ (Start 2009), „EnMap“ (Start 2011) oder die gewerbliche Nutzung von ursprünglich für staatliche Zwecke geplanten Satelliten zu. Die entstehenden Erdfernerkundungsdaten haben eine Qualität, welche bis vor kurzem nur von klassifizierten militärischen Satelliten erzeugt werden konnte. Anders als für den Export der entsprechenden Satelliten oder der damit im Zusammenhang stehenden Technologien gibt es im deutschen Recht zurzeit keinerlei Regelungen, welche das Verbreiten derartiger Daten betreffen; auch das Exportkontrollrecht kennt hierfür keinerlei Beschränkungen. Dennoch waren sich die Partner des TerraSAR-Projektes bei Abschluss des Vertrages der Sicherheitsrelevanz ihres Vorhabens bewusst und haben ihre Tätigkeiten unter den Vorbehalt einer nationalen Datensicherheitspolitik und eines Gesetzes in Umsetzung dieser Politik gestellt.

Neben diesen nationalen Erwägungen wird eine Regelung zur Datensicherheitspolitik auch erforderlich, weil praktisch alle leistungsfähigen Satellitensysteme auf Exportgenehmigungen einzelner kritischer US-Bauteile angewiesen sind. Die USA fordern in diesen Fällen das Vorhandensein von nationalen Regelungen, die Sicherheitsinteressen an Daten berücksichtigen, welche unter Zuhilfenahme der amerikanischen Bauteile gewonnen werden. Die Regelungen dieses Gesetzes vereinfachen das Verfahren für den Import kritischer Bauteile hochwertiger Erdfernerkundungssysteme, da sie den einheitlichen und transparenten Rahmen schaffen, der für einen Umgang mit sicherheitsrelevanten Daten zwingend erforderlich ist.

Eine eigenständige Regelung der von der hochwertigen Erdfernerkundung betroffenen Bereiche ist notwendig, da das geltende Recht diese Sachverhalte nicht erfasst. Eine Ergänzung des Ausfuhrrechts, das einen vergleichbaren Schutzzweck verfolgt und eine Ausfuhr der betreffenden Erdfernerkundungssysteme und der zugrunde liegenden Technologie bereits regelt, würde den Sicherheitsinteressen nicht Genüge tun. Denn diese sind auch bei rein nationalen oder innergemeinschaftlichen Sachverhalten gefährdet. Regelungsbedürftig ist daher nicht die Ausfuhr, sondern das Verbreiten der Daten.

Vertragliche Regelungen mit den betroffenen Unternehmen der Betreiber und Datenanbieter können die Sicherheitsinteressen nicht in vergleichbarer Weise schützen. Eine einheitliche Umsetzung der Datensicherheitspolitik wäre nicht sichergestellt. Zugleich fehlten die Grundlagen, die Betroffenen zum Abschluss und zur Einhaltung der Regelungen zu zwingen bei gleichzeitiger Beachtung von deren freier wirtschaftlicher Betätigung. Es wäre auch in Bezug auf Verbindlichkeit, Durchsetzbarkeit und außenpolitische Signalwirkung kein vergleichbarer Standard gewährleistet.

Die technischen Abläufe im Rahmen der raumgestützten Erdfernerkundung lassen sich vereinfacht wie folgt darstellen: Der Betreiber des Satelliten erzeugt mittels des Kontroll-Bodensegements die Kommandos zur Kommandierung des Orbitalsystems und (selbst oder im Auftrag des Datenanbieters) die Kommandos zur Steuerung der Erdfernerkundungssensoren (als Nutzlast des Orbitalsystems). Hieran knüpft Teil 2 des Gesetzes an. Die Daten werden dann von einem Nutzlast-Bodensegment beim Betreiber oder Datenanbieter empfangen und zum Verbreiten vorbereitet. Die Gewährleistung der Sicherheit in der Handhabung und Aufbewahrung dieser Daten knüpft daher vor

deren Verbreiten beim Betreiber (Teil 2) oder Datenanbieter (Teil 3, Kapitel 1) an.

Ein potenzieller Kunde für Erdfernerkundungsdaten wendet sich an den Datenanbieter. Datenanbieter kann auch der Betreiber des Erdfernerkundungssystems selbst sein. Zwischen dem Datenanbieter und dem Kunden erfolgt das Verbreiten der Daten. Hier setzt Teil 3, Kapitel 2 des Gesetzes an, indem es die Bedienung der Kundenanfrage unter Prüfungs- und Erlaubnisvorbehalt stellt. Bezieht sich der Kundenwunsch auf schon in der Vergangenheit aufgezeichnete Daten, werden diese aus dem Archiv entnommen (gegebenenfalls entsprechend der Kundenwünsche zu dem bestellten Datenprodukt verarbeitet) und an den Kunden übermittelt. Müssen die vom Kunden bestellten Daten neu aufgezeichnet werden, wird der Auftrag zur Erzeugung der Daten an den Betreiber übermittelt, der mit dem Kontroll-Bodensegment eine entsprechende Kommandierung an das Erdfernerkundungssystem übermittelt.

Möchte der Kunde ein neu aufzuzeichnendes Rohdatenprodukt erhalten, kann das Verbreiten auch so erfolgen, dass der Datenanbieter ein Kommando zur Erzeugung der Daten und ein Übertragungskommando über das Kontroll-Bodensegment absendet und das Orbitalsystem die Daten direkt an ein Nutzlast-Bodensegment des Kunden sendet. Zwischen dem Datenanbieter und dem Kunden würde dann lediglich der Schlüssel zum Decodieren der direkt übermittelten Rohdaten ausgetauscht. Dieses direkte Übertragungsverfahren ist im Bereich der Erdfernerkundung seit langem etabliert und wird üblicherweise nur mit besonders großen Kunden, welche über Rahmenverträge entsprechende Vereinbarungen mit dem Anbieter abschließen, angewendet.

II. Lösung

Durch das Gesetz werden vier Verwaltungsverfahren eingerichtet und teilweise mit Mitteilungspflichten versehen. Kernbestandteil ist der unter Nummer 4 dargestellte Erlaubnisvorbehalt zum Verbreiten von Erdfernerkundungsdaten. Da das Regelungsziel aber nur erreicht werden kann, wenn bis zum Verbreiten ein sicherer Umgang mit den Erdfernerkundungsdaten gewährleistet ist, werden technische Anforderungen an das Erdfernerkundungssystem und persönliche Anforderungen an den Betreiber und den Datenanbieter gestellt.

1. Der Betrieb eines hochwertigen Erdfernerkundungssystems bedarf der Genehmigung. Dieser Genehmigungsvorbehalt richtet sich an den Betreiber des Systems, der von dem Datenanbieter verschieden sein kann. Die Genehmigungspflicht dient einerseits dazu, dass das Erdfernerkundungssystem gewisse Sicherungsmechanismen aufweist und durch den Umgang mit diesem und den erzeugten Daten kein Sicherheitsrisiko entsteht. Andererseits sollen Erdfernerkundungssysteme von der Genehmigungspflicht ausgenommen werden, die nicht das Potenzial besitzen, überhaupt Daten zu erzeugen, deren Verbreiten sicherheitsrelevant ist.

   Es werden Auskunftspflichten und Betretens- und Prüfungsrechte bestimmt, um der Behörde die Prüfung der Einhaltung des Gesetzes zu ermöglichen.

2. Der ausländische Erwerb eines Betreiberunternehmens und einer Unternehmensbeteiligung muss vom Erwerber gemeldet werden und kann zum Schutz der Sicherheitsinteressen untersagt werden. Die Übernahme des Betriebs eines hochwertigen Erdfernerkundungssystems bedarf der Erlaubnis.

3. Derjenige, der Daten verbreitet, bedarf einer Zulassung. Die Zulassungsvoraussetzungen gewährleisten parallel zu den Genehmigungsvoraussetzungen des Betreibers, dass der Zugelassene die Daten ordnungsgemäß aufbewahrt und dass der Umgang mit den Daten keine Sicherheitsrisiken zur Folge hat. Die Daten unterliegen einem besonderen Schutzbedürfnis, weil noch keine Sensitivitätsprüfung durchgeführt wurde (vgl. Nummer 4). Auch hier werden Auskunftspflichten sowie Betretens- und Prüfungsrechte etabliert.

4. Das Gesetz verpflichtet den Datenanbieter von Erdfernerkundungsdaten zunächst zu einer eigenverantwortlichen Prüfung jeder Anfrage in Bezug auf Daten eines hochwertigen Erdfernerkundungssystems (Sensitivitätsprüfung). Diese Prüfung dient als Filter und verringert die Anzahl der Anfragen, die einer behördlichen Prüfung zugeführt werden müssen. Die Kriterien sind dabei die Person des Anfragenden und seiner Kunden, das angefragte Zielgebiet, der Informationsgehalt der Daten und die gewünschte Zeitnähe. Das Gesetz bestimmt Kriterien dieser Prüfung, ohne dem Datenanbieter einen eigenen Beurteilungsspielraum zu belassen. Die Ausgestaltung der Kriterien erfolgt durch Rechtsverordnung. Die Prüfung ist zu dokumentieren, um die Einhaltung der gesetzlichen Vorgaben überwachen zu können.

   Erst wenn diese Prüfung des Datenanbieters zu dem Ergebnis kommt, dass die Möglichkeit eines Schadenseintritts gegeben ist, wird ein behördliches Verfahren eingeleitet. Die zuständige Behörde prüft dann auf Antrag des Datenanbieters, ob durch das Verbreiten die Sicherheit der Bundesrepublik Deutschland tatsächlich gefährdet ist.

III. Gesetzgebungskompetenz des Bundes

Die Teile 2 und 3 des Gesetzes, welche die wesentlichen Regelungen darstellen, fallen unter das Recht der Wirtschaft, Artikel 74 Abs. 1 Nr. 11 GG. Denn sie schaffen die gesetzlichen Rahmenbedingungen und Pflichten für die in diesem Bereich tätigen Wirtschaftsunternehmen. Insofern richten sich der Gehalt der Regelungen und deren unmittelbare Wirkung auf einen Gegenstand der konkurrierenden Gesetzgebung. Der darüber hinausgehende Zweck des Gesetzes, die Wahrung außen- und sicherheitspolitischer Interessen Deutschlands, ist bei der Beurteilung der Gesetzgebungskompetenz von nachrangiger Bedeutung.

Die für den Bereich der konkurrierenden Gesetzgebung nach Artikel 72 Abs. 2 GG gebotene Erforderlichkeit einer bundesgesetzlichen Regelung ist in der Wahrung der Rechtseinheit im gesamtstaatlichen Interesse begründet. Denn nicht vorhandene oder unterschiedliche Gesetze auf Länderebene würden eine Rechtszersplitterung mit problematischen Folgen darstellen, die im Interesse sowohl des Bundes als auch der Länder nicht hingenommen werden kann. Ohne eine bundeseinheitliche Regelung wären zum einen die außen- und sicherheitspolitischen Interessen Deutschlands nicht zu schützen. Die Untätigkeit der Länder auf diesem Gebiet und die Tatsache, dass es sich bei diesen

Interessen um einheitliche nationale Interessen des Bundes, welche auch nur von diesem definiert werden können, handelt, machen eine bundesgesetzliche Regelung erforderlich. Zum anderen stellt die Tätigkeit der Satellitenbetreiber und Datenanbieter im gesamten Bundesgebiet einen einheitlichen Lebenssachverhalt dar. Es ist nicht denkbar, dass regionale Unterschiede zu einer unterschiedlichen Beurteilung dieser Tätigkeiten führen und damit eine unterschiedliche Regelung erfordern. Denn einerseits sind die außen- und sicherheitspolitischen Interessen, die mit Hilfe dieses Gesetzes geschützt werden sollen, einheitlich zu beurteilen, andererseits erzeugen Erdfernerkundungssatelliten Daten jedes Punktes der Erdoberfläche. Eine rechtliche Ungleichbehandlung der Satellitenbetreiber und Datenanbieter auf Länderebene würde daher zu Rechtsunsicherheit und damit zu unzumutbaren Behinderungen für den länderübergreifenden Rechtsverkehr führen, da deren Tätigkeit ihrer Natur nach die Grenzen der einzelnen Bundesländer überschreitet.

Teil 4 des Gesetzes enthält Regelungen, für welche eine ausschließliche Gesetzgebungskompetenz des Bundes nach Artikel 73 Nr. 1 GG (Verteidigung) gegeben ist. Hinter diesen Schwerpunkt der Regelungen tritt die ebenfalls gegebene wirtschaftsregelnde Wirkung zurück. Denn die in diesem Teil geregelte vorrangige Bedienung von Anfragen der Bundesrepublik Deutschland dient der Sicherstellung der Versorgung der Streitkräfte und des Bundes im Bündnis-, Verteidigungs-, Notstands- und Spannungsfall.

Teil 6 des Gesetzes enthält die Bußgeld- und Strafbestimmungen. Diese fallen unter Artikel 74 Abs. 1 Nr. 1 GG (Strafrecht) als Gegenstand der konkurrierenden Gesetzgebung.

Teil 7 des Gesetzes ändert das Bundesverfassungsschutzgesetz und das Sicherheitsüberprüfungsgesetz. Der Bund kann bezüglich § 32 eine Kompetenz aus Artikel 73 Abs. 1 Nr. 10b und 10c GG in Anspruch nehmen. Die Kompetenz bezüglich § 33 folgt aus der Natur der Sache, da das Gesetz ausschließlich Sicherheitsbestimmungen für die Bundesverwaltung trifft, die nur durch den Bund selbst erlassen werden können.

Bislang bestehen keine Regelungen im Bereich des Verbreitens von Erdfernerkundungsdaten auf europäischer Ebene. Deutschland ist aufgrund seiner technologischen Spitzenstellung im Bereich der Erdfernerkundung der einzige Mitgliedstaat der Union, in dem derzeit Daten hochwertiger Erdfernerkundungssysteme gewerblich verbreitet werden sollen. Mittelfristig wird dies auch in Frankreich und Italien möglich sein.

IV. Auswirkungen auf den Bundeshaushalt, die Wirtschaft und die Preise

Das Gesetz begründet durch die Schaffung der neuen Verwaltungsverfahren Vollzugsaufwand für den Bund. Für Länder und Kommunen werden keine neuen Aufgaben oder Aufwendungen entstehen.

Bei den zuständigen Behörden sowie den im Verfahren von der zuständigen Behörde eventuell beteiligten weiteren Behörden entsteht Vollzugsaufwand durch Verwaltungsverfahren zur Genehmigung des Betriebs hochwertiger Erdfernerkundungssysteme (einschließlich der Aufsicht des Betreibers), zur Zulassung der Datenanbieter (einschließlich der Aufsichtsaufgaben) sowie zur Erteilung der Erlaubnis zum Verbreiten sensitiver Anfragen. Darüber hinaus können im Einzelfall auch die Erlaubnis zur Übernahme des Betriebs eines Satelliten oder Prüfungen zur Zulässigkeit ausländischer Unternehmensbeteiligung erforderlich werden.

Es ist zu erwarten, dass der Vollzugsaufwand für die Genehmigungen und Zulassungen durch das Bundesamt für Wirtschaft und Ausfuhrkontrolle wegen der in den nächsten Jahren sehr überschaubaren Zahl der Betreiber (ein bis zwei) von Erdfernerkundungssystemen und Datenanbietern (zwei bis zehn) gering bleibt.

Die Abschätzung des Vollzugsaufwands zur Erteilung der Erlaubnis zum Verbreiten sensitiver Datenanfragen durch das Bundesamt für Wirtschaft und Ausfuhrkontrolle hängt von der Zahl entsprechender Anfragen und von der genauen Ausgestaltung der in § 17 Abs. 2 in Verbindung mit der Rechtsverordnung nach Absatz 3 genannten Kriterien der Sensitivitätsprüfung ab. Diese werden durch den Stand der Technik sowie die fachliche und politische Einschätzung der Bundesregierung in Bezug auf die Möglichkeit eines Schadenseintritts für die im Gesetz beschriebenen Schutzgüter bestimmt.

Ausgehend von den in den nächsten Jahren zu erwartenden Erdfernerkundungssystemen und den Erwartungen für die weltweiten Märkte für Erdfernerkundungsdaten kann davon ausgegangen werden, dass die Aufgaben insgesamt mit einem zusätzlichen Personalbedarf von elf Personen durchgeführt werden können. Dies hat Ausgaben von jährlich etwa 0,7 Mio. Euro zur Folge. Der Personalbedarf soll soweit wie möglich durch Überhangpersonal aus der Bundesverwaltung gedeckt werden.

Im Bundesministerium für Wirtschaft und Technologie und beim Bundesamt für Verfassungsschutz entsteht geringer zusätzlicher Aufwand, da weitere Personen eine einfache Sicherheitsüberprüfung benötigen. Die Anzahl wird von den Betreibern und Datenanbietern bestimmt, dürfte aber wegen deren Zahl und dem für die Betroffenen entstehenden Aufwand eher klein anzusetzen sein. Zusätzlich entsteht im Bundesministerium für Wirtschaft und Technologie Personalaufwand infolge der Zuständigkeit für den Erlass der Rechtsverordnungen und gegebenenfalls bei der Prüfung eines ausländischen Erwerbs eines Betreiberunternehmens. Insgesamt ist im Bundesministerium für Wirtschaft und Technologie mit einem Personalbedarf von zwei Stellen zu rechnen. In einer ersten Gesamtbewertung wird davon ausgegangen, dass die Aufgabe beim Bundesamt für Wirtschaft und Ausfuhrkontrolle mit acht zusätzlichen Personen durchgeführt werden kann (zudem werden gegebenenfalls interne Umschichtungsspielräume genutzt).

Beim Bundesamt für Sicherheit in der Informationstechnik wird durch die Prüfung der Sicherheitsverfahren bei Betreiber und Datenanbieter zusätzlicher Aufwand entstehen. Diese Prüfung ist im Genehmigungs- und Zulassungsverfahren sowie anschließend nur im Falle einer Änderung der Sicherheitsverfahren zu leisten. Es kann daher erwartet werden, dass der Vollzugsaufwand gering bleibt. Zudem entsteht einmalig bei der Vorbereitung der Prüfverfahren für

den Fall zusätzlicher Aufwand, dass die Erstellung von Schutzprofilen oder technischen Richtlinien erforderlich ist.

Eine Überprüfung des Personalbedarfs nach zwei Jahren ist vorgesehen.

Für die betroffenen Unternehmen und Einrichtungen wird zusätzlicher Aufwand entstehen. Dieser konzentriert sich auf den einmaligen Aufwand zur Einholung einer Genehmigung bzw. einer Zulassung. Dieser Aufwand wird zur Einrichtung der im Gesetz vorgeschriebenen organisatorischen und technischen Vorkehrungen und Verfahren zur Sicherung des Zutritts und Zugangs, zur Sensitivitätsprüfung und zur Dokumentation entstehen. Darüber hinaus wird im Geschäftsbetrieb bei Datenanbietern zusätzlicher Aufwand durch das Erfordernis zur Durchführung der Sensitivitätsprüfung entstehen; im Einzelfall kann auch die Einholung einer Erlaubnis erforderlich werden.

Der zusätzliche Aufwand wird gering bleiben, weil die Einrichtung der geforderten Vorkehrungen einerseits bereits bei der Planung der Anlagen und des Geschäftsbetriebs berücksichtigt werden können und andererseits in vielen Fällen in ähnlicher Form zum Schutz der Geschäftsinteressen ohnehin von den Unternehmen und Einrichtungen durchgeführt würden. Die zum Verbreiten von Daten geforderten Verfahren sind weitgehend automatisierbar und können in den normalen Geschäftsbetrieb integriert werden. Geringfügige kosteninduzierte Einzelpreisanpassungen lassen sich jedoch nicht ausschließen. Auswirkungen auf die Einzelpreise und das Preisniveau, insbesondere Verbraucherpreisniveau, sind aber nicht zu erwarten.

Das Gesetz regelt das sichere Verbreiten von raumgestützten Erdfernerkundungsdaten unabhängig davon, ob das Verbreiten gewerblichen oder durch eine von der öffentlichen Hand geförderte Einrichtung geschieht. Soweit von der öffentlichen Hand geförderte Einrichtungen betroffen sind, ist aus Gründen der Haushaltstransparenz für diese Einrichtungen keine Gebührenbefreiung für Amtshandlungen der zuständigen Behörde vorgesehen.

Bürokratiekosten durch Informationspflichten entstehen für den Betreiber eines hochwertigen Erdfernerkundungssystems infolge der Dokumentationspflicht des § 5, der Anzeigepflicht des § 6, der Auskunftspflicht des § 7 und der Mitwirkungspflicht im Rahmen einer Betriebsprüfung nach § 8. Den Datenanbieter treffen Informationspflichten infolge der Dokumentationspflicht des § 18, der Anzeigepflicht des § 13, der Auskunftspflicht des § 14 und der Mitwirkungspflicht im Rahmen einer Betriebsprüfung nach § 15. Zusätzlich entstehen Informationspflichten dadurch, dass der Betreiber und der Datenanbieter verpflichtet sind, bestimmte Personen einer einfachen Sicherheitsüberprüfung unterziehen zu lassen. Da mit den beabsichtigten Regelungen sowohl technisch als auch fachpolitisch Neuland betreten wird, ist eine Kostenabschätzung derzeit nicht möglich.

V. Auswirkungen von gleichstellungspolitischer Bedeutung

Auswirkungen von gleichstellungspolitischer Bedeutung sind nicht zu erwarten.

B. Zu den einzelnen Vorschriften

Zu § 1 (Anwendungsbereich)

Zu Absatz 1

In den sachlichen Anwendungsbereich fällt nach Nummer 1 der Betrieb von hochwertigen Erdfernerkundungssystemen. Ein hochwertiges Erdfernerkundungssystem ist ein raumgestütztes Erdfernerkundungssystem mit besonderen Eigenschaften im Sinne von § 2 Abs. 1 Nr. 4 in Verbindung mit § 2 Abs. 2.

Die personelle Hoheitsgewalt wird bestimmt durch die deutsche Staatsangehörigkeit (Nummer 1 Buchstabe a Alternative 1) der natürlichen Person bzw. die Staatszugehörigkeit der juristischen Person. Die deutsche Staatszugehörigkeit erfasst sowohl die Gründung nach deutschem Recht (Nummer 1 Buchstabe a Alternative 2 und 3) als auch den Sitz (Nummer 1 Buchstabe b) einer juristischen Person. Zu den Personenvereinigungen zählen vor allem nichtrechtsfähige Vereine, OHG, KG, GmbH & Co. KG und die GbR. Der territoriale Anwendungsbereich wird durch Nummer 1 Buchstabe c geregelt. Auch wenn ein Erdfernerkundungssystem von einem Ausländer in der Bundesrepublik Deutschland betrieben wird, müssen die nationalen Sicherheitsinteressen gewahrt bleiben. Als Anknüpfungspunkt für die territoriale Hoheitsgewalt für den Betrieb eines Erdfernerkundungssystems wird der Ort gewählt, von dem die tatsächliche Betriebsgewalt über das Raumsegment ausgeübt wird, da der Erdbeobachtungssatellit selbst sich im internationalen Territorium Weltraum (vgl. Artikel II des Vertrages über die Grundsätze zur Regelung der Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraums einschließlich des Mondes und anderer Himmelskörper vom 27. Januar 1967, BGBl. 1969 II S. 1967 ff.) befindet. Die tatsächliche Betriebsgewalt wird gekennzeichnet durch das unveränderbare Absetzen der Befehlsfolgen zur Kommandierung. Da es in Ausnahmefällen vorkommen kann, dass auch Kunden die Möglichkeit eingeräumt bekommen, Sensoren und teilweise das gesamte Orbitalsystem zu kommandieren, und sich der Betreiber nur ein Überschreibungsrecht dieser Befehlsfolgen vorbehält, muss es auf das letztverantwortliche Absetzen ankommen. Der Ort, an dem dies passiert, ist die zentrale Bodenkontrollstation (Kontroll-Bodensegment). Hier besteht die Möglichkeit, jedes Signal noch einmal unveränderbar zu überschreiben.

In den sachlichen Anwendungsbereich fällt nach Nummer 2 der Umgang mit den Daten von hochwertigen Erdfernerkundungssystemen, die im Anwendungsbereich dieses Gesetzes betrieben werden. Der Umgang mit den Daten wird nur bis zu dem Zeitpunkt geregelt, in dem die Daten verbreitet werden.

Der personelle Anwendungsbereich ist entsprechend der Nummer 1 geregelt.

Der territoriale Anwendungsbereich knüpft daran an, dass die für das Verbreiten der Daten wesentlichen Betriebsteile im Bundesgebiet gelegen sind. Unerheblich ist es, wenn sich lediglich ein Archiv oder eine Datenverarbeitungseinrichtung im Bundesgebiet befindet.

Zu Absatz 2

Der Anwendungsbereich des Gesetzes erfasst nicht militärische Erdfernerkundungssysteme. Auch kann oder muss von der Anwendung des Gesetzes abgesehen werden, wenn ein Erdfernerkundungssystem auch in den Anwendungsbereich eines ausländischen Gesetzes über das Verbreiten von Erdfernerkundungsdaten fällt.

Zu Satz 1

Staatliche Satelliten, deren Daten einer adäquaten Geheimhaltung unterliegen, sind von den Bestimmungen dieses Gesetzes ausgenommen. Voraussetzung dieser Ausnahme ist ein staatlicher Betrieb mit militärischen oder nachrichtendienstlichen Aufgaben. Anwendungsfall ist das geplante SAR-Lupe-System des Bundesministeriums der Verteidigung oder mögliche zukünftige Systeme, welche unter die BOC-Vereinbarungen (Besoin Operationelles Communs – Vereinbarungen einiger europäischer Staaten zu Gemeinsamen Anforderungen an Satellitenaufklärung) fallen. Diese Stellen schützen durch Geheimhaltungsverfahren die Daten im Einzelfall gegen unbefugte Kenntnisnahme.

Zu den Sätzen 2 und 3

Es ist nicht ausgeschlossen, dass nach dem Anwendungsbereich dieses Gesetzes der Betrieb eines hochwertigen Erdfernerkundungssystems oder das Verbreiten von Daten nicht nur von der Bundesrepublik Deutschland, sondern auch von einem anderen Staat kontrolliert wird. Es wird die Möglichkeit geschaffen, dass in einem solchen Fall eine deutsche Betriebsgenehmigung nicht eingeholt werden muss, sofern ein vergleichbarer Sicherheitsstandard gewährleistet ist. Erforderlich ist eine abstrakte Vergleichbarkeit der Vorschriften, keine Übereinstimmung im Einzelfall. Derzeit gibt es nur eine US-amerikanische und eine kanadische Regelung. Mittelfristig werden noch einige wenige Staaten hinzukommen. Die mit der Anwendung dieses Gesetzes verbundenen Beschränkungen der gemeinschaftsrechtlichen Dienstleistungsfreiheit sind unter Berücksichtigung des Prinzips der gegenseitigen Anerkennung innerhalb der Europäischen Union gerechtfertigt, weil von der Anwendung dieses Gesetzes abgesehen werden muss, sobald vergleichbare Sicherheitsstandards durch die Rechtsvorschriften eines anderen Mitgliedstaates gewährleistet ist. Bei sonstigen Staaten (Drittstaaten) muss die Vergleichbarkeit in einer völkerrechtlichen Vereinbarung festgestellt werden. Es steht dann im Ermessen der zuständigen Behörde, von der Anwendung abzusehen.

Zu § 2 (Begriffsbestimmungen)

Zu Absatz 1

Die gesetzliche Definition des „Betreibers“ entspricht der im besonderen Verwaltungsrecht üblichen Auslegung. Kennzeichen eines Betreibers sind neben der wirtschaftlichen Verantwortung die rechtliche Verfügungsbefugnis und die tatsächliche Sachherrschaft. Die tatsächliche Sachherrschaft über ein Erdfernerkundungssystem besitzt derjenige, der – über das Kontroll-Bodensegment – in eigener Verantwortung die Befehlsfolgen (Kommandosequenzen) an das Erdfernerkundungssystem absetzt. Dies ist der Fall, wenn die Befehlsfolgen unveränderbar abgesetzt werden können. Der Betreiber ist nicht notwendig der Eigentümer des Erdfernerkundungssystems, da dieser auf die Verfügungsgewalt verzichten kann. Ein „hochwertiges Erdfernerkundungssystem“ ist ein raumgestütztes Erdfernerkundungssystem mit den besonderen Eigenschaften des Absatzes 2. Ein raumgestütztes Erdfernerkundungssystem ist zunächst ein Orbital- oder Transportsystem einschließlich des Bodensegments, mit dem Daten über die Erde erzeugt werden. Orbitalsysteme sind dabei Systeme auf einer Umlaufbahn (Orbit) um die Erde. Typische Orbitalsysteme sind Satelliten oder Raumstationen. Transportsysteme dienen der Verbringung von Orbitalsystemen zu ihrem Einsatzort im Orbit. In Ausnahmefällen können sie aber auch zur Erdfernerkundung eingesetzt werden. Praktisch relevante Transportsysteme sind zurzeit nur das Space-Shuttle oder andere Raumfähren bzw. -gleiter. Die Begriffe des Orbital- und Transportsystems erfassen in Kombination alle zur raumgestützten Erdfernerkundung verwendeten Systeme. Nicht erfasst davon sind Suborbitalsysteme, also Systeme, die keine Erdumlaufbahn erreichen, z. B. Höhenforschungsraketen. Sie überfliegen ein mögliches Zielgebiet nur einmal, so dass keine vergleichbare Sicherheitsgefährdung gegeben ist. Der Begriff des Bodensegments bezeichnet alle technischen Anlagen am Boden, welche zum Betrieb, zum Datenempfang und zur Verarbeitung der Daten des Erdfernerkundungssystems erforderlich sind. Der Begriff des Orbitalsystems umfasst auch Formationen von Satelliten, welche sich in relativ geringem und klar definierten Abstand (wenige 100 Meter oder wenige Kilometer) zueinander befinden und die das Zielgebiet quasi gleichzeitig überfliegen. Solche Formationen erkennt man typischerweise daran, dass die beteiligten Satelliten mit speziellen technischen Ausrüstungen ihre genaue relative Lage zueinander bestimmen und möglicherweise auch regeln können. Ebenfalls erfasst sind Konstellationen (typischerweise ähnlicher) Satelliten. Diese überfliegen ein Zielgebiet mit deutlichem zeitlichen Abstand. Durch die Verarbeitung der Daten kann ein besonders hoher Informationsgehalt erzielt werden.

Der Begriff der „Daten“ umfasst alle von den Sensoren des Erdfernerkundungssystems erzeugten Signale und die daraus gewonnenen oder abgeleiteten Datenprodukte. Es handelt sich um einen spezifischen Begriff, der nur von einem Erdfernerkundungssensor erzeugte Daten beinhaltet und dadurch nur einen kleinen Ausschnitt des allgemein verwendeten Datenbegriffs erfasst. Die Einordnung unter den Datenbegriff ist unabhängig vom Verarbeitungsgrad und der Art der Speicherung oder Darstellung der Daten und schließt daher sowohl analoge Fotos als auch digitale Datenprodukte ein. Der Datenbegriff umfasst beispielsweise zwei- oder mehrdimensionale Datenfelder, die Eigenschaften der Erde mit Raumbezug darstellen, sowie Bilder der Erdoberfläche oder Höhenmodelle. Umfasst sind auch die sog. Rohdaten (Sensordaten mit keinem oder geringem Prozessierungsgrad) und alle daraus abgeleiteten höherwertigen Datenprodukte. Insbesondere bei den digitalen Datenprodukten ist es unerheblich, ob es sich um zweidimensionale Datenfelder (z. B. digitale Schwarzweiß-Fotos), mehrdimensionale Datenfelder (z. B. multi-, super- oder hyperspektrale Daten) oder eine andere Darstellung von raumbezogenen Daten der Erde oder der sie unmittelbar umgebenden Region (d. h. vom Erdinneren, über die Erdoberfläche, Atmosphäre bis etwa zur Ionosphäre) handelt. Eingeschlossen ist auch jede andere Darstellung raumbezogener Daten wie Höhenmodelle, komplexe Radardaten mit Phaseninfor-

mation, interferometrische Daten oder Daten aus Satellitenformationen.

Wegen der Beschränkung auf die Signale eines Sensors ist für den Fall der personenbezogenen Daten eine Ausnahme zugunsten des allgemein verwendeten Datenbegriffs formuliert. Erforderlich ist diese Ausnahme, da die Regelung des betreffenden § 27 eine andere Schutzrichtung hat. Denn sie dient nicht wie die übrigen Vorschriften des Gesetzes dem Schutz vor Gefährdungen der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von Erdfernerkundungsdaten, sondern dem Schutz der Einzelangaben über Personen und Unternehmen. Es findet daher in diesem Zusammenhang der allgemeine, weite Datenbegriff Anwendung, der auch den Datenschutzgesetzen zugrunde liegt.

„Datenanbieter“ ist, wer von einem hochwertigen Erdfernerkundungssystem erzeugte Daten aus dem durch die §§ 4 ff. und 12 ff. gesicherten Bereich herausgibt. Dies kann der Betreiber eines hochwertigen Erdfernerkundungssystems selbst oder ein Nutzungsberechtigter sein, der die Daten ohne Prüfung nach § 17 erhalten hat. Datenanbieter ist nicht, wer Daten weitergibt, die diese Prüfung bereits durchlaufen haben.

Der Begriff des „Sensors“ wird ohne Differenzierung der aktiven und passiven Fähigkeit definiert: Damit sind alle Sensoren umfasst, die ein Nutzlastelement auf, in oder an einem raumgestützten Erdfernerkundungssystem haben. Unerheblich ist, ob der Sensor seine eigene elektromagnetische Strahlung aussendet, um ein Objekt aufzuspüren oder um ein Gebiet zu beobachten, und die von dort reflektierte Strahlung empfängt oder ob er für elektromagnetische Strahlung empfindlich ist, die von dem zu beobachtenden Objekt ausgesandt wird oder von dem Objekt reflektiert wird, aber nicht den Sensor selbst als Quelle hat. Obwohl mittelfristig die elektromagnetischen Strahlungen die einzig praxisrelevanten Strahlungen sein werden, wurden gravimetrische Messfelder berücksichtigt.

„Verbreiten“ ist gesetzlich definiert als Inverkehrbringen oder Zugänglichmachen an Dritte. Dritter ist, wer nicht verpflichtet ist, die Sicherheitsinteressen der Bundesrepublik Deutschland beim Betrieb eines hochwertigen Erdfernerkundungssystems oder beim Umgang mit den Daten bis zum Verbreiten zu schützen. Dies beschränkt den Anwendungsbereich: Daten, die den durch die §§ 4 ff. und 12 ff. gesicherten Bereich des Betreibers eines Erdfernerkundungssystems oder eines Datenanbieters verlassen haben, unterliegen keinen Umgangsbeschränkungen. Denn sie sind durch die im Gesetz etablierten Verfahren bereits auf ihre Eignung zur Gefährdung der Sicherheitsinteressen geprüft. Der Begriff des Zugänglichmachens ist dabei ein Auffangtatbestand und umfasst beispielsweise die einmalige Einsichtnahme durch Dritte oder die eigeninitiative Veröffentlichung der Daten. Die Begrenzung beruht darauf, dass mit dem Verlassen des Bereichs beim Datenanbieter die tatsächliche Möglichkeit endet, umfassende Kontrolle über die Daten zu gewährleisten. Das Risiko unberechtigter Weitergabe ist bei dem Verbreiten an den Kunden bereits zu berücksichtigen.

Zu Absatz 2

Absatz 2 legt in Ausgestaltung von Absatz 1 Nr. 4 abschließend die Kriterien fest, anhand derer zu bestimmen ist, ob ein Erdfernerkundungssystem hochwertig ist. Die Bestimmungen der Rechtsverordnung, die die Kriterien der Sätze 1 und 2 ausfüllen, müssen berücksichtigen, welches technische Potenzial eines Erdfernerkundungssystems die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker oder die auswärtigen Beziehungen der Bundesrepublik Deutschland gefährden kann. Dies erfolgt aufgrund einer aktuellen Bedrohungsanalyse, berücksichtigt aber auch die Erhältlichkeit vergleichbarer Daten auf internationalen Märkten. Denn wenn Daten einer gewissen Qualität an anderer Stelle frei zugänglich sind, besteht ein vergleichsweise geringes Interesse, das Verbreiten von Daten eines deutschen Erdfernerkundungssystems gleicher Qualität Beschränkungen zu unterwerfen.

Die Kriterien sind dem Wandel der Sicherheitsinteressen sowie dem technischen Wandel unterworfen. Die erforderliche Flexibilität ist durch eine Bestimmung im Verordnungswege gewährleistet.

Der Begriff der geometrischen Auflösung bezeichnet die kleinste in den Daten eines Erdfernerkundungssystems trennbare geometrische Einheit auf allen drei Achsen im Raum. Die Erkennbarkeit von Details geometrischer Strukturen, welche anhand der Daten dargestellt werden, hängt direkt mit der geometrischen Auflösung zusammen. Im Falle eines klassischen zweidimensional abbildenden Sensors ergibt sich die geometrische Auflösung aus der kleinsten Fläche (geometrische Einheit) im Zielgebiet, über die das vom Sensor erfasste radiometrische Signal integriert wird, das heißt aus der geometrischen Einheit, welche am Boden innerhalb eines Bildpunktes (Pixel) erfasst wird. Für optische Sensoren kann die geometrische Auflösung im obigen Sinne als Gesichtsfeld oder Öffnungswinkel für einen Pixel (Instantaneous field of view, IFOV) definiert werden. Für Radarsensoren kann der Begriff der geometrischen Auflösung an der Impulse Response Function festgemacht werden. Im Fall eines Sensors, der Daten mit Informationen über die Höhenstruktur des Zielgebietes liefert, umfasst der Begriff auch die erreichbare Höhenauflösung. Oft werden diese Daten als geometrisch zweieinhalb-dimensional oder weniger genau als dreidimensional bezeichnet, da sie zu jedem beobachteten Auflösungselement des Zielgebietes (Pixel) auch eine absolute oder relative Höhenangabe bieten. Durch entsprechende Verarbeitung werden aus solchen Daten digitale Höhenmodelle abgeleitet. Nach heutigem Stand der Technik können solche Daten beispielsweise durch stereoskopische Beobachtung oder interferometrische Verfahren (z. B. InSAR) oder zukünftig durch aktive Rangingverfahren (z. B. LIDAR, Light Detection and Ranging) gewonnen werden. Die Eignung zur Erfassung der Höhenstruktur kann zudem bei in Formation fliegenden Orbitalsystemen vermutet werden (vgl. die Begründung zu § 2 Abs. 1 Nr. 4).

Der Informationsgehalt von Erdfernerkundungsdaten wird nicht nur durch die geometrische Auflösung, sondern maßgeblich auch durch den spektralen Informationsgehalt der Daten bestimmt. Dies trifft aus heutiger Sicht in besonderem Maße für die optischen Sensoren zu, könnte in Zukunft aber auch zunehmend für Radar- bzw. SAR-Sensoren große Bedeutung erlangen. In diesem Zusammenhang werden im Gesetz die spezifischeren Begriffe der „spektralen Abdeckung“ und der „spektralen Auflösung“ genutzt. Der Begriff

der spektralen Abdeckung beschreibt, welcher Spektralbereich vom Sensor insgesamt erfasst werden kann. Spektralbereiche können durch den Frequenz- bzw. Wellenlängenbereich oder durch allgemein genutzte technische Begriffe beschrieben werden. Typische technische Begriffe sind beispielsweise UV (Ultraviolett), VIS (für das menschliche Auge sichtbarer Spektralbereich), NIR (Nahes Infrarot), SWIR (short-wave infrared), TIR (thermisches Infrarot). In der Regel können aus spektraler Information Rückschlüsse über die Materialbeschaffenheit des beobachteten Objektes gezogen werden. Ein hoher spektraler Informationsgehalt, der sich aus der spektralen Abdeckung und der spektralen Auflösung ergibt, kann so insbesondere enttarnende Wirkung haben. Fernerkundungssensoren, deren abgedeckter Spektralbereich in wenige Kanäle aufgeteilt ist, werden als multispektrale Sensoren bezeichnet. Fortschrittliche Multispektralsektoren erkennen Dutzende (superspektrale Sensoren) oder gar hunderte (hyperspektrale Sensoren) von einzelnen Spektralbereichen für jedes einzelne räumliche Pixel. Der Begriff der spektralen Auflösung bezieht sich dabei auf die Fähigkeit eines Sensors, zwischen kleinen Intervallen von Wellenlängen zu unterscheiden – d. h. auf die Breite eines einzelnen Spektralkanals. Die spektrale Auflösung ist besonders bei hyperspektralen Sensoren in Verbindung mit modernen Prozessierungsverfahren von erheblicher Bedeutung.

Bei der radiometrischen Auflösung handelt es sich um die Fähigkeit eines Sensors, kleine Unterschiede bzw. Kontraste in der Intensität der elektromagnetischen Strahlung zu unterscheiden. Im einfachsten Fall eines panchromatischen Sensors (vergleichbar einem Schwarz-weiß-Sensor, der den gesamten für das menschliche Auge sichtbaren Spektralbereich in einem Kanal abdeckt) beschreibt die radiometrische Auflösung, wie viele unterschiedliche Graustufen ein Sensor unterscheiden kann. Da die radiometrische Auflösung sehr eng mit der beobachtbaren Dynamik und dem beobachtbaren Kontrastumfang zusammenhängt, ermöglicht eine hohe radiometrische Auflösung beispielsweise auch die Beobachtung von Details in Schattenregionen einer ansonsten hell beleuchteten Szenerie.

Bei der zeitlichen Auflösung handelt es sich um den zeitlichen Abstand, der zwischen zwei Aufnahmen desselben Gebietes mit einem Sensor liegt; bei Satellitensystemen ist er durch die Parameter der Umlaufbahn und durch eine eventuell vorhandene Schwenkmöglichkeit des Sensors oder des ganzen Satelliten mit dem Sensor vorgegeben. Daten mit hoher Wiederholrate eignen sich vor allem für die Dokumentation dynamischer Vorgänge. Bei optischen Sensoren ist die praktische Sicherheitsrelevanz zurzeit nicht gegeben. Mit dem Aufkommen von Orbitalsystemen mit mehreren Satelliten kann die zeitliche Auflösung allerdings sehr schnell kritisch werden. Insbesondere bei Radar- bzw. SAR-Systemen könnte eine hohe zeitliche Wiederholrate als sicherheitsrelevant eingestuft werden, weil ein geringer zeitlicher Abstand zwischen zwei Beobachtungen desselben Gebietes die sog. Kohärenz begünstigt und damit besonders hochwertige Prozessierungsverfahren ermöglicht.

Mikrowellensensoren sind im cm-Wellenbereich (zwischen ca. 1 mm und 1 m) empfindlich für die von der Erde reflektierte Strahlung. Es kommen passive Systeme wie auch aktive Systeme zum Einsatz. Zu letzteren zählt die Radar-Fernerkundung, die im Vergleich zur Beobachtung im Bereich des sichtbaren Lichtes und des Infrarots andere Möglichkeiten erschließt. Dazu gehören die erhöhte Eindringtiefe der Strahlung in die Erdoberfläche (X-Band, 3-cm-Wellen) sowie die Unabhängigkeit von Witterungsbedingungen, da die Moleküle in der Atmosphäre im Mikrowellenbereich nicht stören. In der raumgestützten Erdfernerkundung werden typischerweise Radarsensoren mit synthetischer Apertur, so genannte SAR-Systeme (Synthetic Aperture Radar) verwendet, weil derartige Systeme eine relativ hohe geometrische Auflösung bei überschaubarer Größe der Radarantenne zulassen.

Obwohl Polarisationsmerkmale auch im optischen Spektralbereich relevant sind, wird nur die Polarisation bei Mikrowellensensoren in Bezug genommen. Gemeint ist dabei die Fähigkeit eines Sensors, bei der Aussendung und beim Empfang zwischen horizontal und vertikal polarisierten Mikrowellen zu unterscheiden. Der Begriff der Phasengeschichte wird meist im Zusammenhang mit Radar-Erdfernerkundungssensoren benutzt und bezeichnet den zeitlichen Verlauf der Signal-Phase, der zur Bildung der „synthetischen Apertur“ bei der Prozessierung eines SAR-Bildes bekannt sein muss. Die Phasengeschichte entsteht bei der Erdfernerkundung durch Radarsensoren mit synthetischer Apertur sowie bei einigen anderen Erdfernerkundungssensoren. Hier entstehen beim kohärenten Empfang des Rückstreusignals aus dem Zielgebiet nicht nur einfache Intensitätssignale, sondern ein so genanntes komplexes Signal. Je nach Art der Prozessierung der Rohdaten des SAR-Erdfernerkundungssensors im Nutzlastbodensegment können Datenprodukte entstehen, in welchen diese Phasengeschichte erhalten bleibt. Spezielle Verfahren erlauben es, den besonderen Informationsgehalt durch Nutzung der Amplituden- und der Phaseninformation auszuwerten. So kann die Phaseninformation in interferometrischen Auswerteverfahren genutzt werden, um beispielsweise Höheninformation, Höhenänderungen oder Geschwindigkeiten von beobachteten Zielen zu gewinnen.

Zu § 3 (Genehmigung)

Zu Absatz 1

Der Betrieb eines hochwertigen Erdfernerkundungssystems bedarf der Genehmigung. Die Hochwertigkeit bestimmt sich nach der Eignung des Sensors, Daten mit einem besonders hohen Informationsgehalt zu erzeugen. Maßgeblich ist die technische Möglichkeit, nicht eine beabsichtigte Verwendung. Hochwertig ist ein Erdfernerkundungssystem, wenn die Daten aufgrund ihrer Qualität geeignet sein können, die außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland zu gefährden.

Die Genehmigung gewährleistet den sicheren Betrieb des Erdfernerkundungssystems. Denn wenn die Kommandierung des Satelliten, die Kommandierung der Sensoren zur Erzeugung der Daten oder die Übermittlung der Daten vom Satelliten zum Bodensegment nicht sicher sind, kann die Sicherheit zu einem späteren Zeitpunkt nicht mehr hergestellt werden und eine Kontrolle bei dem Verbreiten nach § 17 ff. liefe ins Leere.

Zu Absatz 2

Die Möglichkeit nachträglicher Änderungen der Genehmigung findet sich in zahlreichen Regelungen des besonderen

Verwaltungsrechts. Im Interesse der Rechtssicherheit des Betreibers ist sie entsprechend § 49 Abs. 2 des Verwaltungsverfahrensgesetzes (VwVfG) auf die Fälle der geänderten Sach- oder Rechtslage beschränkt. Wegen der Bedeutung der Schutzgüter dieses Gesetzes wurde jedoch auf das zusätzliche Erfordernis der Gefährdung des öffentlichen Interesses verzichtet.

Aus Gründen der Formen- und Verfahrensklarheit ist der Betreiber mit der Genehmigungserteilung auf die Möglichkeit der Änderung hinzuweisen.

Zu Absatz 3

Nicht umfasst von der Genehmigung nach § 3 Abs. 1 ist beispielsweise die nach § 55 des Telekommunikationsgesetzes (TKG) erforderliche Frequenzzuteilung sowie die nach § 56 TKG erforderliche Übertragung der Orbit- und Frequenznutzungsrechte durch die Bundesnetzagentur. Darüber hinaus wäre auch eine allgemeine Betriebserlaubnis nicht von der Genehmigung umfasst: § 3 zielt im Ergebnis nämlich lediglich auf anwendungsspezifische Elemente des Satellitenbetriebs (hier Erdfernerkundung). Eine allgemeine Betriebserlaubnis basierend auf Artikel VI des Vertrages über die Grundsätze zur Regelung der Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraums einschließlich des Mondes und anderer Himmelskörper vom 27. Januar 1967 (BGBl. 1969 II S. 1967 ff.) würde die Einhaltung der völkerrechtlichen Verpflichtungen der Bundesrepublik Deutschland voraussetzen. Eine solche Betriebserlaubnis, die auch der Haftungsprävention dient, ist vom deutschen Gesetzgeber bislang jedoch nicht eingeführt. Satz 2 stellt klar, dass durch die Genehmigung weder über die datenschutzrechtliche Zulässigkeit der beabsichtigten Tätigkeit noch über die Vereinbarkeit mit sonstigen Rechten Dritter, z. B. § 22 ff. des Kunsturhebergesetzes (KUG), entschieden wird. Aufgrund des Standes der Technik sind jedoch derzeit und in absehbarer Zukunft diese persönlichen Rechte nicht berührt.

Zu Absatz 4

Dieser Negativattest (Null-Bescheid) dient der Sicherheit des Betreibers. Es wird festgestellt, dass ein Fernerkundungssystem nicht hochwertig ist und daher ohne Genehmigung nach § 3 in Betrieb genommen werden kann. Der Negativtest steht dem Betreiber sowohl vor Start und Inbetriebnahme seines Erdfernerkundungssystems als auch des Betriebs auf Antrag offen. Damit wird der Tatsache Rechnung getragen, dass sich die Kriterien, welche an den Sensor und den Informationsgehalt der Daten gestellt werden, im Laufe der Jahre ändern. Denn der Markt erhältlicher Daten wird sich nach den Erfahrungen der vergangenen Jahre und angesichts der voranschreitenden technischen Entwicklung auch außerhalb des Militärs deutlich erweitern. Damit werden, bis zu einer gewissen Grenze, auch die Anforderungen an einen hohen Informationsgehalt der Daten etwas steigen, was eine Änderung der Rechtsverordnung nach § 2 Abs. 2 zur Folge haben wird. Für ein Erdfernerkundungssystem, das nach einer Änderung nicht mehr hochwertig ist, hat sich die Genehmigung erledigt. Mit Hilfe dieser Regelung kann der Betreiber dies feststellen lassen.

Zu § 4 (Genehmigungsvoraussetzungen)

Zu Absatz 1

Die Einhaltung der Genehmigungsvoraussetzungen gewährleistet einen sicheren Betrieb des Erdfernerkundungssystems sowie einen sicheren Umgang des Betreibers mit den Daten.

Die Zuverlässigkeit des Betreibers (Nummer 1) wird anhand einer Einschätzung der zukünftigen Erfüllung seiner Pflichten beurteilt. Die Erfüllung ist zweifelhaft, wenn der Antragsteller in der Vergangenheit gegen Vorschriften dieses Gesetzes oder sachnaher anderer Gesetze (z. B. AWG, GewO oder die §§ 80 bis 109k StGB) verstoßen hat oder entsprechende Anhaltspunkte bestehen. Berücksichtigt werden auch Verstöße gegen allgemeine Gesetze, die Rückschlüsse auf sein berufliches Verhalten zulassen, beispielsweise Verstöße gegen steuer-, sozial- und arbeitsschutzrechtliche Bestimmungen und unvorteilhafte Angaben zu Fragen entsprechend § 13 Abs. 1 Nr. 13 bis 17 des Sicherheitsüberprüfungsgesetzes (SÜG). Wenn es sich beim Betreiber um eine juristische Person handelt, sind deren gesetzliche Vertreter sowie deren Eigentümer oder Anteilseigner maßgeblich. Anhand einer Prognose wird die dauerhafte Erfüllung der gesetzlichen Pflichten abgeschätzt. Die Zuverlässigkeit wird tätigkeits- und schutzgutbezogen ausgelegt. Es ist der zuständigen Behörde möglich, im Genehmigungsverfahren umfassende Angaben zum Beispiel zu den Beteiligungsverhältnissen zu fordern, um zu einer möglichst belastbaren Beurteilung der Zuverlässigkeit zu kommen. Dabei sind im Rahmen der Prognoseentscheidung die gesetzlichen Dokumentations- und Auskunftspflichten des Betreibers insofern zu berücksichtigen, als dass sie geeignet sind, die dauerhafte Erfüllung der gesetzlichen Pflichten zu erhöhen. Neben diesen gesetzlichen Pflichten können dem Betreiber im Einzelfall weitere Pflichten auferlegt werden, wenn diese zur Sicherstellung seiner Zuverlässigkeit erforderlich sind, § 36 VwVfG. Im Falle von Pflichtverletzungen durch den Betreiber ist anhand der geänderten Sachlage eine neue Bewertung seiner Zuverlässigkeit erforderlich. Die Behörde kann gegebenenfalls Maßnahmen anordnen, um einer mangelnden Zuverlässigkeit abzuhelfen.

Nummer 2 stellt die positive Kontrolle über das Orbitalsystem und deren Ausübung vom Bundesgebiet aus sicher. Dazu werden die bezeichneten Befehlsfolgen vor der Übertragung zum Satelliten beispielsweise durch eine Authentisierung gesichert. Diese Voraussetzung ermöglicht es, jederzeit den Zugriff auf denjenigen zu behalten, der die sicherheitsrelevanten Teile des Orbitalsystems innerhalb eines Erdfernerkundungssystems verantwortlich kommandiert. Zugleich ermöglicht das Erfordernis einer starken Authentisierung der Befehlsfolgen, dass an der Übermittlung auch Bodensegmente beteiligt sein können, die sich nicht im Bundesgebiet befinden. Die Einbeziehung solcher Bodensegmente ist aus technischen Gründen von Interesse und dürfte vielfach genutzt werden, da ein Orbitalsystem ja nach seiner Bahn und Position einen Zeitraum von bis zu wenigen Tagen benötigt, bis es wieder in das Sichtfeld eines Bodensegments auf deutschem Territorium gelangt.

Die Kommandierung des Orbitalsystems betrifft das Kommandosystem des Telemetrie, Tracking und Commands (TT&C). Die Betriebsüberwachung der Satelliten-Untersysteme (Telemetrie) und die Bahnvermessung (Tracking)

muss nicht besonders geschützt werden. Nur die Kommandosysteme beeinflussen den Betriebsablauf des Orbitalsystems derart, dass eine Sicherheitsgefährdung im Sinne des Gesetzes entstehen kann.

Bei Nummer 2 geht es – im Gegensatz zu Nummer 3 – nur um den Daten-Uplink, also die Kommandos, die an das Orbitalsystem gesendet werden. Die dritte Alternative der Nummer 2 betrifft nur die „Befehlsfolgen zur Steuerung der Datenübermittlung“, das heißt das Kommando des Bodensegments an den Bordcomputer des Raumsegments, die Daten aus dem Speicher abzusenden. Nicht betroffen ist die Datenübermittlung selbst (der vom Kommando ausgelöste Vorgang). Die Datenübermittlung unterfällt der Nummer 3.

Das Gesetz verwendet für die Weitergabe von Daten zwei unterschiedliche Begriffe: Übermitteln und Verbreiten. Übermittlung ist der übergeordnete Begriff für jede Art der Übertragung oder Weitergabe von Daten, so dass ein Verbreiten einen bestimmten Fall der Übermittlung darstellt. Vor dem Verbreiten erfolgt die Übermittlung von Daten vom Raumsegment eines Erdfernerkundungssystems (typischerweise eines Satelliten) an eine Bodenempfangsstation einer nach dem Gesetz verpflichteten Person, zwischen verschiedenen Teilen eines Bodensegments (z. B. von der Bodenempfangsstation zur Verarbeitungsstation oder zum Archiv) oder zwischen Bodensegmenten verschiedener nach dem Gesetz verpflichteter Personen. Hier sind Sicherheitsanforderungen im Umgang mit den Daten vor deren Verbreiten gestellt (§§ 4 ff. und 12 ff.). Werden die Daten von den nach dem Gesetz verpflichteten Personen an Personen weitergegeben, die nicht mehr nach dem Gesetz verpflichtet sind, so werden die Daten verbreitet (§ 17 ff.). Für den Fall, dass die Daten direkt an eine Bodenstation des Kunden übermittelt werden (vgl. A. I. am Ende), ist diese Übermittlung zugleich ein Verbreiten an den Kunden. Eine Übermittlung in Form der Weitergabe durch den Kunden an Dritte nach einem Verbreiten wird durch das Gesetz nicht beschränkt; falls die Weitergabe jedoch aus anderen Gründen beschränkt ist, wird dies nach § 17 Abs. 3 Satz 2 berücksichtigt.

Anstatt eine eigene Prüfung des Veränderungsschutzes einzuführen, wird in Nummer 2 auf eine Prüfung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verwiesen. Das BSI erstellt eine technische Richtlinie, in die geeignete Schutzprofile einzubeziehen sind, vgl. § 25 Abs. 2.

Nach Nummer 3 muss der Schutz der Datenübermittlung gewährleistet sein. Damit wird ein umfassender Schutz der Daten erreicht, die sich beim Betreiber befinden und die noch nicht an den Datenanbieter übermittelt (an diesen werden die gleichen Anforderungen gestellt, vgl. § 12) und verbreitet worden sind. Es wird sichergestellt, dass Erdfernerkundungsdaten nicht anderen Personen als dem Satellitenbetreiber oder dem Datenanbieter zugänglich sind. Die Übertragung der Daten beinhaltet die Übermittlung vom Orbitalsystem an ein Bodensegment (Kontroll-Bodenbodensegment oder Nutzlast-Bodensegment) und die Übertragung zwischen zwei Bodensegmenten (Nutzlast-Bodensegment des Betreibers zu Nutzlast-Bodensegment des Datenanbieters). Es handelt sich hier um den Daten-Downlink sowie die erdgebundene Übertragung der Daten, bevor es zur Prüfung und zum Verbreiten der Daten kommt.

Die erforderlichen Maßnahmen nach Nummer 4 stellen den Schutz der Betriebsräume und -anlagen beim Betreiber sicher. Es wird dabei zwischen dem Zutritt und dem Zugang unterschieden. Der Zutritt betrifft die Anwesenheit von Personen in bestimmten Betriebsräumen. Es muss ausgeschlossen sein, dass Unbefugte sich dort aufhalten. Der Zugang regelt die Gewährung von Nutzungsmöglichkeiten der betreffenden Anlagen, beispielsweise durch Schlüssel oder Codes. Das Gesetz bestimmt die erforderlichen Sicherheitsvorkehrungen nicht im Einzelnen, sondern bestimmt nur das Ziel. Der Betreiber hat die Möglichkeit, geeignete technische und organisatorische Maßnahmen zu entwickeln und im Genehmigungsverfahren mit der Behörde abzustimmen. Die Einrichtung von effektiven Maßnahmen der Zugangskontrolle wird in der Praxis von erheblicher Bedeutung sein. Denn die Sicherheit wird weniger von demjenigen gefährdet, der sich unberechtigt körperlichen Zutritt zu den Anlagen und dann den Zugang zu den Daten verschafft; bedeutsamer werden Schutzvorkehrungen gegen elektronisches Eindringen sein.

Zu Absatz 2

Neben dem materiellen Schutz der Betriebsräume und Anlagen vor unbefugtem Zutritt und Zugang nach Absatz 1 Nr. 4 müssen die zugangsberechtigten Personen auch sicherheitsüberprüft sein (Innenschutz). Die Sicherheitsüberprüfung ermöglicht die Einschätzung der Zuverlässigkeit derjenigen Personen, welche aufgrund ihrer Stellung die Möglichkeit haben, persönlich die materiellen Schutzvorkehrungen zu umgehen. Denn eine solche Umgehung würde ebenso wie ein unbefugter Zutritt oder Zugang zu einem unkontrollierten Verbreiten von Daten führen.

Zuständig ist das Bundesministerium für Wirtschaft und Technologie, vgl. § 24 Abs. 2. Die Bearbeitung der Sicherheitsüberprüfung ist für den Antragsteller kostenfrei.

Zu § 5 (Dokumentationspflicht)

Die Dokumentationspflicht ermöglicht die Überprüfung der bestehenden Sicherheitsmaßnahmen und die Aufdeckung von Verstößen. Die Aufbewahrungspflicht endet nach fünf Jahren. Der Zeitraum von fünf Jahren entspricht dem des § 3a der Außenwirtschaftsverordnung (AWV) und berücksichtigt die strafrechtliche Verjährung nach § 78 Abs. 3 Nr. 4 des Strafgesetzbuchs (StGB) von fünf Jahren für Straftaten nach § 29 dieses Gesetzes. Infolge einer üblichen Lebensdauer der Satelliten von drei bis sieben Jahren und des mit zunehmendem Alter abnehmenden Gefährdungspotenzials der Satellitendaten ist mit der fünfjährigen Aufbewahrungsfrist ein hinreichender Schutz der Sicherheitsinteressen gewahrt.

Zu § 6 (Anzeigepflicht)

Zu Absatz 1

Der Betreiber wird verpflichtet, Veränderungen von Tatsachen anzuzeigen, die für die Erteilung der Genehmigung maßgeblich waren. Diese Anzeigepflicht dient der Ausübung der behördlichen Aufsicht. Verstöße gegen diese gesetzliche Pflicht des Betreibers können Maßnahmen der Behörde zur Folge haben.

Nummer 1 betrifft Fälle, in denen sich beim Betreiber Tatsachen ändern, die dieser zur Eintragung in das Handels- oder Vereinsregister nach den Vorschriften des HGB, AktG,

GmbHG, BGB oder UmwG anmelden muss, ergänzt um weitere Anzeigepflichten. Eine entsprechende Pflicht für Aktiengesellschaften besteht nicht; eine solche wäre insbesondere unter Berücksichtigung von Streubesitz und freiem Börsenhandel nicht praktikabel. Die Anzeigepflicht gegenüber der zuständigen Behörde besteht zusätzlich zur Anmeldepflicht im Handelsregister. Damit kann die zuständige Behörde sofort Kenntnis der Änderungen erlangen und gegebenenfalls unmittelbar reagieren. Denn Änderungen beispielsweise bezüglich der Person eines Geschäftsführers oder Gesellschafters oder bezüglich des Sitzes könnten die Sicherheitsinteressen gefährden. Die Änderung solcher Tatsachen beim Betreiber beeinflusst folglich auch die Bewertung von dessen Zuverlässigkeit, so dass die zuständige Behörde gegebenenfalls nachträgliche Anordnungen treffen könnte. Der zusätzliche Aufwand des Betreibers zur Anzeige neben der Anmeldung zum Handelsregister ist gering.

Die zuständige Behörde hat darüber hinaus die Möglichkeit, Einsicht in das Handels- oder Vereinsregister zu nehmen.

Nummer 2 berücksichtigt das Risiko, dass die positive Kontrolle über das Erdfernerkundungssystem nicht mehr sichergestellt werden kann, nachdem beispielsweise die Verschlüsselung gebrochen worden ist (vgl. § 4 Abs. 1 Nr. 2).

Nummer 3 betrifft Änderungen der betrieblichen Organisation des Betreibers, die sich im sicherheitsrelevanten Bereich bewegen.

Zu Absatz 2

Die Regelung dient der Nachvollziehbarkeit der Verbreitungswege der Daten. Es lässt sich überprüfen, dass keine Daten den gesicherten Bereich des Betreibers oder Anbieters ohne Sensitivitätsprüfung verlassen.

Zu § 7 (Auskunftspflicht)

Die umfassende Auskunftspflicht ist erforderlich, da die Einhaltung der gesetzlichen Bestimmungen nicht allein durch Straf- und Bußgelddrohung gesichert werden kann. Ermöglicht wird eine präventive Überwachung; der Verdacht eines Verstoßes gegen Regelungen dieses Gesetzes ist nicht erforderlich. Die Auskunftspflicht ist begrenzt auf die Sicherstellung der Einhaltung des vorliegenden Gesetzes und der zu diesem Gesetz erlassenen Rechtsverordnungen. Eine weitergehende Auskunft kann berechtigterweise verweigert werden. Ergänzt wird die Auskunftspflicht durch eine Nachschau im Geschäftsbetrieb nach § 8 und durch die Regelung des § 6, der den Genehmigungsinhaber zu einem aktiven Vorgehen in den dort genannten Fällen verpflichtet. Die Auskunftspflicht ermöglicht es der Behörde aber auch, unabhängig von einem konkreten Anlass zeitraumbezogene Auskünfte zu verlangen. Die Regelung entspricht der im Gewerberecht üblichen Regelung des § 29 Abs. 1, 3 der Gewerbeordnung (GewO). Absatz 2 regelt ein Auskunftsverweigerungsrecht.

Zu § 8 (Betretens- und Prüfungsrechte)

Die Anzeige- und Auskunftspflichten des Betreibers werden durch Betretens- und Prüfungsrechte der Behörde ergänzt, um eine wirksame Kontrolle zu ermöglichen. Im Unterschied zum gewerberechtlichen Recht auf Nachschau, § 29 Abs. 2 GewO, wird das Betretens- und Prüfungsrecht nicht auf Eingriffe außerhalb der Geschäftszeiten ausgedehnt. Diese können nach allgemeinem Gefahrenabwehr- oder Strafprozessrecht vorgenommen werden. Der Verweis auf die Abgabenordnung (AO) ermöglicht der zuständigen Behörde die Einsicht in die gespeicherten Daten und den Zugang zu den Datenverarbeitungssystemen (§ 200 AO i. V. m. § 147 Abs. 6 AO). Zugleich erhöht sich die Rechtssicherheit der Betroffenen infolge des Verweises auf die genau ausgestalteten Regelungen der Abgabenordnung. Zusätzlich werden eine automatische Auswertung ermöglicht und die Überlassung von Datenträgern geregelt. Dies ist erforderlich, da die Betreiber zur erforderlichen Dokumentation voraussichtlich Datenverarbeitungsanlagen einsetzen werden. Eine Prüfung der geschäftlichen Unterlagen, welche zu einer wirksamen Kontrolle des Betreibers erforderlich ist, ist in herkömmlicher Papierform sowohl für den Auskunftspflichtigen als auch für die Behörde mit höherem Aufwand verbunden. Bei der Wahrnehmung der eingeräumten Befugnisse sind die Vorschriften des Bundesdatenschutzgesetzes, insbesondere § 9 Satz 1 und § 20 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG), zu beachten.

Zu § 9 (Maßnahmen der zuständigen Behörde)

Maßnahmen der Behörde sind möglich im Falle von Pflichtverletzungen des Betreibers. Die Pflichten können sich aus dem Gesetz selbst (§§ 5 bis 8), der Genehmigung oder einer nachträglichen Auflage ergeben. Diese Pflichten konkretisieren die außen- und sicherheitspolitischen Interessen, deren Schutz dieses Gesetz verfolgt. Die Verhältnismäßigkeit einer behördlichen Maßnahme ist daran zu messen.

Die Regelbeispiele des Absatzes 2 sind nicht abschließend. Nummer 1 benennt eine Maßnahme, die vor allem dann möglich ist, wenn die direkte Datenübertragung an ein Bodensegment im Ausland mit Sicherheitsrisiken verbunden ist. Nummer 2 ermöglicht die Fortsetzung des Betriebs unter Einsatz eines geeigneten Sonderbeauftragten. Denn falls ein Betreiber keine Gewähr mehr für einen sicheren Betrieb bietet, kann der Satellit nicht ungesteuert im Weltraum treiben: Er könnte Rechtsgüter Dritter schädigen. Zusätzlich haftet die Bundesrepublik Deutschland für Schäden, die durch privat betriebene Satelliten verursacht sind, Artikel VII des Vertrages über die Grundsätze zur Regelung der Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraums einschließlich des Mondes und anderer Himmelskörper vom 27. Januar 1967 (BGBl. 1969 II S. 1967 ff.). Daher muss gewährleistet sein, dass ein geeigneter Betreiber (Sonderbeauftragter) vorübergehend den ordnungsgemäßen Betrieb sicherstellt. Die Geeignetheit des Sonderbeauftragten bestimmt sich nach seiner Eignung zum Betrieb eines Erdfernerkundungssystems, insbesondere unter Beachtung der Vorschriften nach diesem Gesetz. Soweit dies möglich ist, hat er den Betrieb im Interesse des Genehmigungsinhabers weiterzuführen.

Die Regelung des § 9 ist nicht abschließend. Allgemeine ordnungsrechtliche Eingriffsermächtigungen gelten neben § 9.

Zu § 10 (Erwerb von Unternehmen und Unternehmensbeteiligungen; Betriebsübernahme)

Zu Absatz 1

Die Vorschrift stellt sicher, dass die Kontrolle der Datenquelle (Erdfernerkundungssystem, insbesondere der Satellit) im Einflussbereich dieses Gesetzes verbleibt oder die durch eine Verschiebung begründete Sicherheitsgefährdung geprüft wird. Denn mit einer Verschiebung der Beteiligungsrechte auf natürliche oder juristische Personen außerhalb der Hoheitsgewalt der Bundesrepublik Deutschland verlieren die Regelungen des Gesetzes faktisch ihre Wirkung (Sperrminorität bzw. Einfluss auf die Geschäftspolitik). Dadurch könnten Daten dieses Erdfernerkundungssystems verbreitet werden, die nicht eine Prüfung nach oder entsprechend Teil 3 des Gesetzes durchlaufen haben.

Es handelt sich um eine ausnahmsweise erforderliche Beschränkung der Kapitalverkehrsfreiheit, wie sie bislang nur von § 52 AWV aufgestellt ist. § 52 AWV begrenzt die Beschränkung restriktiv auf Unternehmen, die Güter der Kriegswaffenliste herstellen oder entwickeln oder Verschlüsselungsprodukte zur Wahrung des nationalen Geheimschutzes herstellen. Regelungsziel der außenwirtschaftsrechtlichen Norm ist die Erhaltung der politischen und militärischen Handlungsfähigkeit sowie der Bündnisfähigkeit der Bundesrepublik Deutschland. Die Beschränkung nach § 10 dieses Gesetzes verfolgt vergleichbare Sicherheitsinteressen. Von Erdfernerkundungssystemen oder deren Daten selbst geht keine originäre Sicherheitsgefährdung aus. Wirkungen von Waffen, militärische Wirkungen oder politische Drohungen können aber durch Erdfernerkundungsdaten erheblich verstärkt werden. Sie besitzen daher mehr als nur militärisches Potenzial. Sie betreffen unmittelbar die politische und militärische Handlungsfähigkeit sowie die Bündnisfähigkeit der Bundesrepublik Deutschland. Dieser Verstärkungseffekt wird dadurch erhöht, dass deutsche Forschungseinrichtungen und deutsche Industrie bei der Entwicklung und Herstellung von Erdfernerkundungssensoren eine technologische Spitzenstellung einnehmen; nur wenige Staaten verfügen über eine ähnliche Qualität an Erdfernerkundungssystemen, mit denen ein solcher Verstärkungseffekt erzielt werden kann.

Eine ausländische Kapitalbeteiligung muss weder bei der Beantragung noch später schädlich sein. Es ist aber erforderlich, dass jeder Neu- bzw. Zuerwerb von ausländischem Einfluss, der zu einer (Gesamt-)Beteiligung von über 25 Prozent der Stimmrechte der Behörde gemeldet wird. Diese nimmt dann eine (erneute) Prüfung der Zuverlässigkeit vor.

Die Regelung entspricht weitgehend § 52 AWV. Dies ist eine eng begrenzte Ausnahme zur Kapitalverkehrsfreiheit mit abgestimmten und ausgewogenen Schwellenwert- und Anrechnungsvorschriften. Diese sollen unverändert in dieses Gesetz eingehen.

Meldepflichtig ist die ausländische natürliche oder juristische Person oder nichtrechtsfähige Personenvereinigung, welche die Beteiligung erwirbt. Diese kann sich zwar außerhalb des deutschen Hoheitsgebietes befinden. Jedoch ist eine Anknüpfung an diese erforderlich, da nur dort Kenntnis vorhanden ist, ob die 25-Prozent-Schwelle überschritten ist. Hinzu kommt, dass die Zuverlässigkeit des Erwerbers entscheidungserheblich ist. Die Meldepflicht eines Ausländers wirft verschiedene Schwierigkeiten auf (z. B. ggf. Auslandszustellung), die nach allgemeinem Verwaltungsrecht zu lösen sind.

Die Vorschrift stellt eine Beschränkung des Kapitalverkehrs aus Gründen der öffentlichen Sicherheit nach den Artikeln 56, 58 des EG-Vertrages dar. Das Bundesministerium für Wirtschaft und Technologie hat im Einzelfall die staatlichen Sicherheitsinteressen und die Freiheit des Kapitalverkehrs abzuwägen und auch die wirtschaftliche Existenz des betroffenen Unternehmens gebührend zu berücksichtigen. Im Rahmen der Entscheidung sind Auflagen für das Rechtsgeschäft möglich. Damit können auch Fälle gelöst werden, in denen der Betrieb eines hochwertigen Erdfernerkundungssystems nur einen Teil des Rechtsgeschäfts betrifft.

Zu Absatz 2

Eine Sicherheitsgefährdung kann nicht nur entstehen, wenn Einfluss auf das Unternehmen ausgeübt wird, welches ein Erdfernerkundungssystem betreibt, sondern kann in noch höherem Maße entstehen, wenn das Erdfernerkundungssystem selbst übernommen wird.

Die Übernahme des Betriebs eines hochwertigen Erdfernerkundungssystems kann die Sicherheitsinteressen der Bundesrepublik Deutschland beeinträchtigen. Erfolgt die Übertragung des Betriebs innerhalb Deutschlands, mithin innerhalb des Anwendungsbereichs dieses Gesetzes, so ist auch der Betrieb durch den neuen Betreiber genehmigungspflichtig nach § 3. Insoweit ist keine Regelung erforderlich. Wenn der neue Betreiber nicht mehr in den Anwendungsbereich des Gesetzes fällt, verhindert Absatz 2, dass der neue Betreiber des Systems keinen Sicherheitseinschränkungen unterliegt. Denn mangels Ausfuhr (der Satellit ist bereits im Orbit) liegt in diesem Fall kein Exportsachverhalt vor. Damit würde ohne die Regelung des Absatzes 2 die Möglichkeit eröffnet, dass Kunden, die nach den Anforderungen dieses Gesetzes keine Daten bekommen könnten, den Betrieb eines im Weltraum befindlichen Fernerkundungssatelliten übernehmen könnten, ohne dass die Bundesrepublik Deutschland eine rechtliche Möglichkeit der Untersagung hat. Anknüpfungspunkt ist der Betreiberwechsel, nicht der Eigentümerwechsel. Geht das Eigentum (z. B. durch Leasing oder Sicherungsübereignung an eine Bank) über, ohne dass der Besitz (Betriebsgewalt) wechselt, so besteht kein Sicherheitsrisiko. Anders als in Absatz 1 ist der Betreiberwechsel erlaubnispflichtig. Denn mit der Betriebsübernahme können vollendete Tatsachen geschaffen werden. Es wird an dieser Stelle ein Gleichlauf mit dem Exportkontrollrecht hergestellt. Der Export eines Erdfernerkundungssystems oder von Teilen eines solchen wäre auf der Erde genehmigungspflichtig.

Zu § 11 (Zulassung)

Wer Daten eines hochwertigen Erdfernerkundungssystems verbreitet, ist Datenanbieter und bedarf einer Zulassung. Das Verbreiten von Daten solcher Erdfernerkundungssysteme, die nicht hochwertig sind, sowie solcher Erdfernerkundungssysteme, die nicht im Anwendungsbereich des Gesetzes liegen, ist dagegen keinen Regelungen unterworfen.

Die Zulassung unterliegt denselben Voraussetzungen wie die Betreibergenehmigung bezüglich der Sicherheit im Umgang mit den Daten. Sie berechtigt den Inhaber zum

Umgang mit den Daten, ohne dass eine Prüfung nach § 17 Abs. 1, § 19 Abs.1 Satz 1 oder 2 erforderlich ist. Der Betreiber eines hochwertigen Erdfernerkundungssystems verbreitet keine Daten, solange sich die Daten in einem Bereich befinden, der durch die §§ 4 ff. und 12 ff. geschützt ist.

Wer die Daten aus diesem Bereich heraus verbreiten möchte, bedarf der Zulassung und muss bei dem Verbreiten § 17 ff. beachten. Der Begriff der „Zulassung“ dient ausschließlich der Abgrenzung von der Genehmigung nach § 3.

Wer Daten verbreitet, die nicht im Anwendungsbereich dieses Gesetzes erzeugt worden sind, bedarf keiner Zulassung. Denn die Sicherheit kann dadurch, dass ein Deutscher beim Vertrieb von Daten eines ausländischen Erdfernerkundungssystems Sicherheitsanforderungen unterworfen wird, nicht erhöht werden. Solange ausländische Anbieter der Daten desselben Systems nicht denselben Anforderungen unterliegen, verfehlt eine nationale Regelung der Sicherheit ihr Ziel. Der Markt ist international und die Datenübertragung kaum zu unterbinden. Bei Anwendung der Regelungen auf Daten ausländischer Satelliten wäre daher die Wirkung ausschließlich eine Schlechterstellung des in Deutschland zugelassenen Anbieters.

Zu Absatz 2 vgl. § 3 Abs. 2.

Zu § 12 (Zulassungsvoraussetzungen)

Die Regelungen des Absatzes 1 Nr. 1 und 2 entsprechen den Regelungen des § 4 Abs.1 Nr. 1 und 4.

Nummer 3 sichert die Übermittlung der Daten zwischen verschiedenen Bodensegmenten eines Datenanbieters oder an einen anderen Datenanbieter. Ebenso wie in § 4 Nr. 3 ist das Verfahren vom BSI zu prüfen und für geeignet zu erklären.

Nummer 4 gewährleistet ein sicheres Verbreiten der Daten zu den Anfragenden. Betroffen ist auch das unmittelbare Verbreiten der Daten durch den Betreiber (auf Anweisung des Datenanbieters) an den Kunden für den Fall, dass die Daten direkt vom Satelliten zu einer Bodenstation des Kunden übermittelt werden. Der Datenanbieter muss ein sicheres Verbreiten, beispielsweise durch eine Verschlüsselung, garantieren. Das Gesetz formuliert jedoch im Unterschied zu § 4 Nr. 3 keine zwingenden Verfahren für das Verbreiten der Daten, da die zu verbreitenden Daten bereits die Sensitivitätsprüfung und gegebenenfalls die behördliche Prüfung durchlaufen haben. Das Verbreiten muss dem Stand der Technik entsprechen. Mögliche Anpassungen sind vom Datenanbieter vorzunehmen und können von der zuständigen Behörde angeordnet werden.

Zu Absatz 2 vgl. § 4 Abs. 2.

Zu § 13 (Anzeigepflicht)

Die Nummern 1 und 2 entsprechen der Regelung des § 6 Nr. 1 und 2. Nummer 3 dient dem Schutz des Datenbestandes. Durch die Anzeigepflicht wird sichergestellt, dass durch Betriebseinstellung keine Gefährdungen von den Daten, beispielsweise durch Aufgabe der Schutzmaßnahmen, ausgehen.

Zu § 14 (Auskunftspflicht)

Die Regelung entspricht § 7.

Zu § 15 (Betretens- und Prüfungsrechte)

Die Regelung entspricht § 8.

Zu § 16 (Maßnahmen der zuständigen Behörde)

Satz 1 entspricht der Regelung des § 9 Abs. 1. Das Regelbeispiel des Satzes 2 Nr. 1 betrifft den typischen Fall, dass infolge des technischen Fortschritts die Sicherungsverfahren beim Verbreiten der Daten überholt sind und angepasst werden müssen. Das Regelbeispiel des Satzes 2 Nr. 2 ermöglicht eine vorübergehende Nutzungsuntersagung.

Die Regelung ist nicht abschließend. Allgemeine ordnungsrechtliche Ermächtigungen gelten neben § 16.

Zu § 17 (Sensitivitätsprüfung)

Zu Absatz 1

Die Sensitivitätsprüfung nach § 17 Abs. 1 Satz 1 ist eine Vorprüfung im Sinne einer Erheblichkeitsprüfung durch den Datenanbieter.

Die Kriterien der Sensitivitätsprüfung des Datenanbieters lassen sich jedoch wegen der Vielzahl der zu verknüpfenden Parameter im Gesetz nicht konkretisieren. Es wird dem Datenanbieter daher ein Verfahren vorgegeben, anhand dessen die Sensitivität eindeutig festgestellt werden kann. Mit der Sensitivitätsprüfung wird dem Datenanbieter zum Zwecke der Erleichterung des Verwaltungsverfahrens und der Entbürokratisierung ein wesentlicher Teil des Schutzes der Sicherheitsinteressen der Bundesrepublik Deutschland übertragen. Alternativ käme nur eine behördliche Einzelfallprüfung jeder Anfrage in Betracht. Dies ist mit einem angemessenen Aufwand nicht zu leisten. Diese dem Datenanbieter überlassene Prüfung muss – im Sinne der Sicherheit – von der Behörde überprüft werden. Aus diesen Gründen erfährt die Sensitivitätsprüfung eine ausführliche Regelung in § 17 f.

Nur ein Datenanbieter ist verpflichtet, Sensitivitätsprüfungen vorzunehmen. Datenanbieter nach § 11 ist derjenige, der Daten eines hochwertigen Erdfernerkundungssystems verbreitet. Damit ist sichergestellt, dass über den Datenanbieter hinaus keine allgemeinen Umgangsbeschränkungen bestehen. Zugleich ist die Sensitivitätsprüfung anfragebezogen, d. h. die Sensitivitätsprüfung muss auch durchgeführt werden, wenn die angefragten Daten bereits früher einmal an einen anderen Anfragenden verbreitet worden sind.

Zu Absatz 2

Es werden die Kriterien bestimmt, anhand derer sich die Sensitivität der Anfrage ergibt. Die Kriterien müssen in ihrem Zusammenspiel miteinander betrachtet werden. Eine isolierte Betrachtung eines einzelnen Aspekts ist nicht hinreichend. Die Zusammenschau der Kriterien muss die Möglichkeit (nicht: Wahrscheinlichkeit) eines Schadenseintritts für die genannten Schutzgüter ergeben. Damit wird der Tatsache Rechnung getragen, dass an dieser Stelle, an der der Datenanbieter die Sensitivität prüft, noch keine Gefahr (Wahrscheinlichkeit eines Schadenseintritts) gegeben sein muss. Aus der Möglichkeit eines Schadenseintritts resultiert zunächst nur eine Notwendigkeit einer behördlichen Prüfung. Innerhalb dieser behördlichen Prüfung wird dann festgestellt, ob eine Gefahr gegeben ist. Die Kriterien gemäß Absatz 2 dienen also nicht der abschließenden Beurteilung

der Gefahrenkonstellation, sondern der Ermittlung der Fälle, die einer behördlichen Prüfung unterzogen werden.

Die Ausfüllung der in Absatz 2 abschließend genannten Kriterien ist wegen deren Veränderbarkeit (teilweise innerhalb weniger Tage oder Stunden) nur im Verordnungswege zu leisten.

Die Zusammenschau erfolgt in Ansehung der Person des Anfragenden. Diese ist dem Datenanbieter immer bekannt. Die Person des Anfragenden kann das Ergebnis der Sensitivitätsprüfung entscheidend beeinflussen. Eine Anfrage beispielsweise eines Verteidigungsministeriums eines NATO-Mitgliedstaates kann unsensitiv sein, während die identische Anfrage einer sonstigen Person sensitiv ist.

Unter Berücksichtigung der Gegebenheit, dass für viele Anfragen der unmittelbar Anfragende die Daten nicht ausschließlich für sich behält (beispielsweise der Anfragende ist Zwischenhändler, Direct Access Customer, Direct Access Partner oder nur Strohmann), sollen auch die Personen berücksichtigt werden, die bestimmungsgemäß mit den Daten in Kontakt kommen. Es ist aber nicht ausgeschlossen, dass der Antragsteller in seiner Anfrage das Kriterium der Personen, die bestimmungsgemäß mit den Daten in Kontakt kommen, offenlässt; beispielsweise wenn der Anfragende als Wiederverkäufer handelt und seine Kunden nicht benennen kann oder nicht benennen möchte. Das Offenlassen eines Kriteriums führt dazu, dass an dessen Stelle alle Möglichkeiten zu berücksichtigen sind, bzw. die für die Bewertung nachteiligste Möglichkeit. Denn die Zusammenschau muss nicht, sondern soll die Personen berücksichtigen, die bestimmungsgemäß mit den Daten in Kontakt kommen. Wird beispielsweise der Kunde eines zugelassenen Anbieters nicht offen gelegt, wird die Anfrage dahin gehend bewertet, dass der Verbleib der Daten unbestimmt ist und somit vom negativsten denkbaren Fall auszugehen ist und die Möglichkeit eines Schadenseintritts steigt. Dies kann dazu führen, dass in solchen Fällen Datenanfragen, die nach den anzulegenden Kriterien als sensitiv zu bewerten sind, ohne Offenlegung der endgültigen Datenempfänger von einer Übermittlung ausgeschlossen sind. Jedoch führt ein Offenlassen allein weder in der Sensitivitätsprüfung noch in der behördlichen Prüfung zu einer Untersagung des Verbreitens.

Die Beurteilung, ob die Möglichkeit eines Schadenseintritts gegeben ist, erfolgt bezogen auf den einzelnen Datensatz. Dies bedeutet jedoch nicht, dass der Datensatz zur Prüfung vorliegen muss. Die Beurteilung lässt sich anhand der Metadaten durchführen. Die Metadaten erlauben eine abstrakte Beschreibung des konkreten Datensatzes und eine Prüfung der Zulässigkeit der Weitergabe dieses Datensatzes bereits vor der Beobachtung des Zielgebiets durch den Satelliten. Zudem muss der Datenanbieter niemals einen Datensatz der Behörde offenlegen. Erfolgt eine Weitergabe der Rohdaten an den Kunden, so ist der Informationsgehalt derjenige, welcher bei einer bestmöglichen Prozessierung zu erreichen ist.

Satz 3 bestimmt, dass der Datenanbieter die Identität des Kunden prüfen muss. In geeigneter Weise erfolgt die Prüfung, wenn sich der Datenanbieter einen amtlichen Ausweis oder ein vergleichbares Dokument, bei Geschäftskunden beispielsweise einen Auszug aus dem Handelsregister, vorlegen lässt. Zugleich hat der Datenanbieter vom Anfragenden eine Liste der Personen zu verlangen, die mit den Daten in Kontakt kommen sollen. Ist der Anfragende selbst nur Zwischenhändler, so sind dies seine Kunden. Insoweit wird dem Datenanbieter aber keine Prüfungspflicht auferlegt. Er muss lediglich die Nennung verlangen. Sanktionen drohen nur im Falle eines bewussten Verstoßes gegen die Aufforderung zur Nennung.

Zu Absatz 3

Die Bestimmung der Grenzwerte der Kriterien des Absatzes 2 Satz 1 und 2 erfolgt durch Rechtsverordnung. Satz 2 bestimmt abschließend, welche Tatsachen und Erwägungen bei Bildung dieser Grenzwerte maßgeblich sind. Grundlage ist die aktuelle Sicherheitslage. Das Bundesministerium für Wirtschaft und Technologie stellt bei Beurteilung der Sicherheitslage das Einvernehmen mit denjenigen Ministerien her, deren Tätigkeit in direkten Bezug zu den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland steht. Aber auch andere Behörden (beispielsweise das Bundeskanzleramt oder nachgeordnete Behörden wie das Bundesamt für Sicherheit in der Informationstechnik oder das Bundeskriminalamt) sind gehalten, ihre Erkenntnisse und Sicherheitsinteressen an die zuständige Behörde weiterzugeben. Von Bedeutung sind ebenfalls die internationalen Verpflichtungen gegenüber verbündeten Staaten. Dies sind die Mitgliedstaaten der Europäischen Union, die NATO-Bündnispartner und die (nach den politischen Grundsätzen der Bundesregierung für den Export von Kriegswaffen und sonstigen Rüstungsgütern vom 19. Januar 2000) NATO-Gleichgestellten Staaten Australien, Japan, Neuseeland und die Schweiz. Vorhandene (ausländische) Regelungen, an die ein Kunde seinerseits gebunden ist, sind ebenfalls zu berücksichtigen, um das Verbreiten von Daten einer an sich sensitiven Anfrage zu ermöglichen, wenn absehbar ist, an wen eine weitergehende Verteilung erfolgen kann. Schließlich ist auch die Verfügbarkeit vergleichbarer Daten auf internationalen Märkten einzubeziehen, um die Konkurrenzfähigkeit des Anbieters nicht zu schwächen, wenn ein wirksamer Schutz der Sicherheitsinteressen ohnehin nicht möglich ist.

Satz 3 verpflichtet den Verordnungsgeber nicht nur, die Kriterien des Absatzes 2 auszufüllen, sondern auch ein Verfahren zu bestimmen, nach dem diese zu prüfen sind. Denn die Kriterien sind in einer Zusammenschau zu prüfen. Der Verordnungsgeber muss daher eine Verknüpfung der Kriterien vorgeben.

Die Anforderungen des Satzes 4 gewährleisten, dass der Datenanbieter sicher weiß, ob ein bestimmter Datensatz verbreitet werden darf oder als sensitiv zunächst der behördlichen Prüfung zuzuführen ist. Dadurch ist eine schnelle und fehlerfreie Durchführung der Sensitivitätsprüfung möglich.

§ 17 erfordert in der Rechtsverordnung nach Absatz 3 ein hohes Maß an Flexibilität. Auch wenn nicht zu erwarten ist, dass sich die Kriterien oder die Kombinatorik sehr häufig ändern, ist ein rasches Handeln erforderlich, wenn sie sich ändern. Um dem Datenanbieter zu ermöglichen, sich bereits vor einer Änderung der Rechtsverordnung auf geänderte Kriterien einzustellen, kann die zuständige Behörde einen Hinweis nach Satz 5 erteilen.

Die Bestimmungen der Kriterien und Parameter der Sensitivitätsprüfung und die einzelnen Grenzwerte stehen jedermann zur Einsicht offen. Denn nicht nur der Datenanbieter

muss sie kennen, sondern auch der Kunde. Andernfalls ist keine sinnvolle Beratung von Seiten des Datenanbieters möglich, wenn beispielsweise ein kritisches Gebiet angefragt wird und die Anfrage auch mit leicht veränderten Kriterien zur Zufriedenheit des Kunden bedient werden kann. Infolgedessen enthalten die Kriterien der Sensitivitätsprüfung keinesfalls Informationen, die ihrerseits selbst geheimschutz- oder sicherheitsrelevant sein könnten. Solche Informationen hat nur die zuständige Behörde zur Entscheidung über die Erlaubnis auf Bedienung einer Anfrage gemäß § 19.

Satz 6 ermächtigt zu einer Subdelegation. Vorgesehen ist, dass der Rahmen von der ermächtigten Stelle vorgegeben wird und eine Ermächtigung der nach § 24 zuständigen Behörde möglich ist.

Zu § 18 (Dokumentationspflicht)

Eine umfassende Dokumentationspflicht ist erforderlich, um die eigenverantwortliche Prüfung des Datenanbieters beaufsichtigen zu können. Die Aufzählung in Absatz 1 Satz 2 ist abschließend. Der Auftrag auf Erzeugung von Daten nach Absatz 1 Satz 2 Nr. 4 umfasst den Auftrag des Datenanbieters an den Betreiber des Erdfernerkundungssystems zur Beobachtung eines Zielgebiets zu einem bestimmten Zeitpunkt mit einem bestimmten Sensorbetriebsmodus.

Die Fünfjahresfrist des Absatzes 2 entspricht der Regelung des § 5.

Zu § 19 (Erlaubnis)

Zu Absatz 1

Nur die Anfragen, für die nach Prüfung des Datenanbieters gemäß § 17 die Sensitivität festgestellt ist, müssen der zuständigen Behörde zur Prüfung vorgelegt werden. Alle anderen Anfragen können vorbehaltlos bedient werden.

Satz 2 ergänzt die Erlaubnispflicht um die Fälle, in denen der Datenanbieter eigeninitiativ Daten verbreitet. Es ist nicht auszuschließen, dass Daten eines hochwertigen Erdfernerkundungssystems auch ohne Anfrage verbreitet werden. In diesem Fall kann keine Sensitivitätsprüfung durchgeführt werden. Denn diese beinhaltet Elemente des Anfragenden, Anfragezeitpunkt etc. In einem solchen sonstigen Fall ist jedes Mal eine Erlaubnis erforderlich.

Zu Absatz 2

Die Schutzgüter greifen auf die Zweckbestimmungen des Außenwirtschaftsrechts (insbesondere § 7 Abs. 1 AWG) zurück. Die Nutzung von Erdfernerkundungssystemen und das Verbreiten damit erzeugter Daten kann sowohl für die innere und äußere Sicherheit der Bundesrepublik Deutschland als auch für die Sicherheit verbündeter wie auch dritter Staaten von Bedeutung sein. Die Erlaubnis wird nur erteilt, wenn eine Gefährdung der wesentlichen Sicherheitsinteressen nicht vorliegt, wenn das friedliche Zusammenleben der Völker nicht gestört ist und wenn die auswärtigen Beziehungen nicht erheblich gestört sind. Bleiben Zweifel an der Gefährdung, so kann die Behörde die Erlaubnis verweigern. Es handelt sich um unbestimmte Rechtsbegriffe, die anhand der aktuellen Sicherheitslage auszulegen sind. Dabei ist ein Gleichlauf mit der Auslegung derselben unbestimmten Rechtsbegriffe in § 7 Abs. 1 AWG beabsichtigt.

Anstelle einer Versagung kann die Behörde das Verbreiten der Daten auch unter Auflagen erlauben. Als solche kommen beispielsweise in Frage die Bedienung der sensitiven Anfrage erst nach angemessener Zeitverzögerung, die Verpflichtung zum Abschluss einer verbindlichen Vereinbarung zwischen dem Datenanbieter und dem Kunden über den Verwendungszweck (ggf. mit der Verpflichtung zur Vereinbarung einer Vertragsstrafe oder anderweitige Durchsetzung), die Weitergabe der Daten an Dritte unter dem Vorbehalt einer erneuten Prüfung durch die zuständige Behörde, die Erzeugung der Daten nur in einem bestimmten Sensorbetriebsmodus, die Übermittlung der Daten nur an bestimmte Bodensegmente oder auch das Verbreiten der Daten nur mit einem verringertem Informationsgehalt.

Zu den Absätzen 3 und 4

Eine behördliche Entscheidung innerhalb einer kurzen Frist ist ein wesentliches Interesse des Datenanbieters, da eine Anfrage vielfach nur innerhalb kurzer Zeit von Interesse ist.

Die Regelung des Absatzes 4 entspricht der des § 3 Abs. 3.

Zu § 20 (Sammelerlaubnis)

Diese Vorschrift eröffnet die Möglichkeit, Vorschaubilder und Miniaturansichten von Daten als Katalogdaten sowie Anfragen eines Kunden auf dasselbe Zielgebiet in wiederkehrenden Abständen allgemein zu bescheiden.

Nummer 1 ermöglicht es dem Datenanbieter, Vorschaubilder bzw. Miniaturansichten (im technischen Umfeld „Browse Images“ genannt) mit stark reduziertem Informationsgehalt in einem Datenkatalog zu veröffentlichen, ohne dass eine Erlaubnis nach § 19 Abs. 1 Satz 2 erforderlich wäre. Vorschaubilder bzw. Miniaturansichten sind Datenprodukte, die durch eine Verarbeitung entstehen, welche sich durch eine verringerte Auflösung, eine verringerte Farbtiefe oder eine zusätzliche verlustbehaftete Kompression auszeichnet. Sie entstehen neben dem Datenprodukt, welches der Datenanbieter eigentlich verbreiten will. Metadaten sind die zentralen Informationen eines Datensatzes, wie in § 18 Abs. 1 Satz 2 Nr. 8 aufgelistet. Vorschaubilder bzw. Miniaturansichten und Metadaten sind ein wichtiges Hilfsmittel für den potenziellen Kunden, um vor einer Anfrage (Bestellung) einen Eindruck von den Daten und deren Eignung für eine bestimmte Aufgabe beurteilen zu können. Die zuständige Behörde muss den Informationsgehalt bestimmen, den ein Vorschaubild bzw. eine Miniaturansicht maximal haben darf. Dies sollte sich an der Wertung der Rechtsverordnung nach § 2 Abs. 2 orientieren, und wird üblicherweise deutlich geringer sein als in dieser Rechtsverordnung festgelegt.

Bei Nummer 2 handelt es sich um ein privilegiertes Verfahren für Datenanbieter, die in einem erheblichen Umfang an bestimmte Kunden liefern. Neben der Sammelerlaubnis ist keine Einzelerlaubnis mehr erforderlich. Sollten im Verlauf des Verbreitens der Daten Tatsachen eintreten, nach denen die zuständige Behörde bei einer Einzelfallerlaubnis nach § 19 eine Erlaubnis nicht erteilt hätte, so kann sie die Sammelerlaubnis widerrufen. Praktisch relevant ist dies insbesondere, wenn sich die aktuelle Sicherheitslage ändert oder die Zuverlässigkeit aufgrund Fehlverhaltens des Erlaubnisinhabers bei der Ausführung des Verbreitens der Daten entfällt.

Zu § 21 (Verpflichtung des Datenanbieters)

Die Regelungen des § 21 ff. sind wegen ihres engen Bezuges zu den Fragen der Sicherheit bei dem Verbreiten von Daten hochwertiger Erdfernerkundungssysteme in das Gesetz aufgenommen worden. Die gesetzlichen Verpflichtungen des Betreibers eines hochwertigen Erdfernerkundungssystems sowie des Datenanbieters lassen sich an dieser Stelle in geeigneter Weise ergänzen. Das Regelungsziel dieses Gesetzes, der Schutz vor Gefahren, die durch die Nutzung von Erdfernerkundungssystemen im Weltraum sowie der auf diesem Wege erzeugten Daten entstehen, ist zu berücksichtigen. Zur Abwehr anderer Gefahren lässt sich eine Verpflichtung zur Einräumung der Nutzung von raumgestützten Erdfernerkundungssystemen im öffentlichen Interesse nur aus allgemeinen Grundsätzen herleiten. Das Gesetz zählt daher abschließend Fälle auf, in denen eine Anfrage (zeitlich) vorrangig zu behandeln ist. Es handelt sich dabei um die im Grundgesetz genannten Fälle des Verteidigungsfalls, des Spannungsfalls, des inneren Notstands und des NATO-Bündnisfalls. Daneben ist der Fall einer Gefährdung von deutschen zivilen oder militärischen Kräften im Auslandseinsatz aufgenommen. Die Unterstützung durch vorrangige Bedienung ist beschränkt auf das Bestehen einer gegenwärtigen Gefahr. Gegenwärtig ist eine Gefahr, wenn das schädigende Ereignis, zum Beispiel ein feindlicher Angriff, unmittelbar bevorsteht. Die Gegenwärtigkeit der Gefahr ist Voraussetzung, da insbesondere Kräfte der Bundeswehr während eines Auslandseinsatzes typischerweise Gefahren ausgesetzt sind. Zu deren Abwehr und zum allgemeinen Schutz können Erdfernerkundungsdaten eingesetzt werden, jedoch nicht aufgrund gesetzlicher Eingriffe beim Datenanbieter oder Satellitenbetreiber. „Vorrangig“ bedeutet, dass die Anfrage zum angefragten Zeitpunkt vor jeder anderen Anfrage bedient werden muss.

Zu § 22 (Verpflichtung des Betreibers)

Der Betreiber des raumgestützten Erdfernerkundungssystems führt die Erdfernerkundung durch; er kommandiert den Satelliten mit dem Ziel der Erzeugung der Daten. Das Vorrecht der Bundesrepublik Deutschland gilt daher nicht nur gegenüber dem Zugelassenen, sondern auch gegenüber dem Betreiber, um zu verhindern, dass eine Anfrage zum Beispiel aufgrund vertraglicher beschränkter Rechte des Datenanbieters gegenüber dem Betreiber nicht vorrangig bedient wird. Diese Verpflichtung des Betreibers lässt den üblichen Vertriebsweg der Daten unberührt. Nur wenn es nicht möglich ist, diesen Vertriebsweg einzuhalten, kann die Anfrage auch direkt beim Betreiber erfolgen. In diesem Fall benötigt der Betreiber dann keine Zulassung nach § 11.

Zu § 23 (Vergütung)

Die vorrangige Bedienung der Anfrage sowie die vorrangige Erzeugung von Daten geben der Bundesrepublik Deutschland ein zeitliches Vorrangrecht. Dieses lässt den Vergütungsanspruch des Betreibers oder Datenanbieters unberührt. Die Vergütung soll dem Marktpreis entsprechen. Das ist der Preis, der ohne zeitlichen Konflikt mit der Ausführung einer anderen Anfrage oder dem Ausführen eines anderen Beobachtungsauftrags zu bezahlen gewesen wäre. Der Marktpreis bemisst sich nach den üblichen Entgeltforderungen des Betreibers oder Datenanbieters und nach dem Preis, den andere Marktteilnehmer für vergleichbare Leistungen verlangen.

Ein über den Vergütungsanspruch hinausgehender Anspruch des Betreibers oder Datenanbieters zum Ausgleich von Schadenersatzansprüchen, die andere Kunden aufgrund nicht oder verspätetet ausgeführter Anfragen möglicherweise gegen ihn haben, ist ausgeschlossen.

Zu § 24 (Zuständigkeit)

Zu Absatz 1

Zuständig ist das Bundesamt für Wirtschaft und Ausfuhrkontrolle, soweit nichts anderes bestimmt ist. Das Bundesamt für Wirtschaft und Ausfuhrkontrolle ist eine bereits existierende, sachnahe Behörde. Denn es hat regelmäßig über Exportanträge für Erdfernerkundungssatelliten zu entscheiden. Die Abwägungen, ob der Export eines ganzen Satelliten die deutschen Sicherheits- und außenpolitischen Interessen gefährdet, entsprechen in weiten Bereichen denen, ob das Verbreiten der Daten eines solchen Satelliten eine Gefahr darstellen könnte. Es wird dadurch ermöglicht, in der Anwendung des AWG und des SatDSiG eine gewisse Synchronisation sicherzustellen, um u. a. eine Schlechterstellung eines in Deutschland ansässigen Vertreibers von Erdfernerkundungsdaten gegenüber einem ausländischen Käufer eines deutschen Erdfernerkundungssatelliten bzw. umgekehrt zu verhindern. Dabei findet eine enge Abstimmung mit den für die Exportkontrolle zuständigen Ressorts statt.

Zu Absatz 2

Zuständige Stelle für die Durchführung der Sicherheitsüberprüfungen nach § 4 Abs. 2 und § 12 Abs. 2 ist das Bundesministerium für Wirtschaft und Technologie. Diese Zuständigkeit entspricht den Regelungen des Sicherheitsüberprüfungsgesetzes.

Zu Absatz 3

Entsprechend der Regelung des § 52 AWV ist zuständige Behörde für die Untersagung des Erwerbs eines Unternehmens oder einer Unternehmensbeteiligung nach § 10 Abs. 1 Satz 4 das Bundesministerium für Wirtschaft und Technologie.

Zu § 25 (Verfahren)

Die Schriftform kann entsprechend § 3a VwVfG durch die elektronische Form ersetzt werden. Die frühzeitige Beteiligung des Bundesamtes für Sicherheit in der Informationstechnik stellt sicher, dass die erforderlichen Sicherheitsverfahren nach § 4 Abs. 1 Nr. 2 und 3 einer hinreichenden Prüfung unterzogen werden.

Das Schriftformerfordernis für Verwaltungsakte nach diesem Gesetz dient der Rechtssicherheit des Antragstellers. Dadurch unterliegt ein Verwaltungsakt, insbesondere die Versagung der Erlaubnis auf Bedienung einer Anfrage auf Verbreiten, der Begründungspflicht, § 39 VwVfG. Die wesentlichen Gründe sind anzugeben. Dabei werden jedoch die Geheimhaltungsbedürftigkeit bestimmter Tatsachen berücksichtigt und die Begründungspflicht insoweit eingeschränkt. Deren Inhalt und Umfang richten sich nach den Besonderheiten des jeweiligen Rechtsgebietes und den Umständen des Einzelfalls. Die Begründung muss wegen des

Gebots des effektiven Rechtsschutzes, Artikel 19 Abs. 4 GG, so einleuchtend sein, dass ein Gericht sie unter Berücksichtigung der rechtstaatlichen Belange noch als triftig erkennen kann, ohne andererseits geheimhaltungsbedürftige Tatsachen unmittelbar oder mittelbar preiszugeben. Ein Hinweis auf die Geheimhaltungspflicht und deren Notwendigkeit ist damit ausreichend.

Zu § 26 (Gebühren und Auslagen)

Die Ausführung des Gesetzes ist gebührenpflichtig. Die Gebühren und Auslagen sind grundsätzlich dem Kostendeckungsprinzip unterworfen. Darüber hinaus wird der Verordnungsgeber auch die Bedeutung, den wirtschaftlichen Wert oder den Nutzen, den die Amtshandlung für den Kostenpflichtigen hat, angemessen berücksichtigen. Dadurch ist gewährleistet, dass die Gebühr an Inhalt und Umfang der Rechtstellung ausgerichtet ist, welche die gebührenpflichtige Amtshandlung dem Einzelnen vermittelt. Der Grundsatz der Verhältnismäßigkeit verlangt, dass die Verwaltungsgebühren nicht so hoch festgesetzt werden, dass sie abschreckend wirken und im Einzelfall ein Missverhältnis zwischen Gebühr und Leistung entsteht; dies bedeutet, dass der Begünstigte durch die Gebühren nicht unangemessen belastet wird.

Soweit von der öffentlichen Hand geförderte Einrichtungen betroffen sind, ist aus Gründen der Haushaltstransparenz für diese Einrichtungen keine Gebührenbefreiung für Amtshandlungen der zuständigen Behörde vorgesehen. Insoweit fördert diese Regelung die verursachergerechte Veranschlagung von Haushaltsmitteln.

Für Amtshandlungen im Rahmen einer nach diesem Gesetz erforderlichen Sicherheitsüberprüfung werden keine Gebühren und Auslagen erhoben. Insoweit gelten die Regelungen des Sicherheitsüberprüfungsgesetzes.

Zu § 27 (Übermittlung von personenbezogenen Daten, Betriebs- und Geschäftsgeheimnissen)

Ziel der Regelung ist ein präventiver Austausch von personenbezogenen Daten, um mögliche Gefährdungen der Sicherheitsinteressen der Bundesrepublik Deutschland durch das Verbreiten von Geoinformationsdaten mit hohem Informationsgehalt (im Sinne von § 2 Abs. 2 dieses Gesetzes) frühzeitig zu erkennen, sowie die Verhütung und Verfolgung von Straftaten. Ebenso wie die entsprechende Regelung des AWG weitet Absatz 1 Satz 2 die Voraussetzungen, unter denen Informationen und personenbezogene Daten an den BND (Bundesnachrichtendienst) weitergegeben werden können, unter Hinweis auf das BND-Gesetz aus. Es handelt sich um eine datenschutzrechtliche Spezialnorm (§ 15 BDSG). Absatz 3 erstreckt den durch die Absätze 1 und 2 gewährleisteten Schutz personenbezogener Daten auf die ebenso schutzbedürftigen Betriebs- und Geschäftsgeheimnisse und trägt damit dem Interesse der Betreiber und Datenanbieter an der Geheimhaltung wettbewerbsrelevanten unternehmerischen Wissens Rechnung.

Zu § 28 (Ordnungswidrigkeiten)

Die Regelung eröffnet die Möglichkeit, Verstöße gegen formelle und materielle Ge- und Verbote dieses Gesetzes als Ordnungswidrigkeiten zu ahnden, sofern sie nicht in besonders schwerwiegenden Fällen kriminelles Unrecht darstellen.

Eine über die Mittel des Verwaltungsrechts hinausgehende Bußgeldbewehrung ist erforderlich, da die Missachtung der gesetzlichen Bestimmungen die Gefährdung der außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland ermöglicht. Es handelt sich dabei um hochrangige Schutzgüter, deren Verletzung einen erheblichen innen- und außenpolitischen Schaden nach sich ziehen kann. Insbesondere der präventive Charakter einer Androhung von Bußgeld (und Geld- oder Freiheitsstrafen nach § 29) ist geeignet zur Befolgung der gesetzlichen Vorschriften aufzurufen.

Tatbestände des Absatzes 1 sind bei Vorsatz oder Fahrlässigkeit erfüllt; die Nummern 1 bis 5 beziehen sich auf Handeln ohne Erlaubnis, Genehmigung bzw. Zulassung sowie die Meldepflicht und sind mit einer Geldbuße bis zu fünfhunderttausend Euro bewehrt. Die Nummern 6 bis 8 betreffen Prüfungs- und Dokumentationsverpflichtungen und sind mit einer Geldbuße bis zu fünfzigtausend Euro bewehrt. Die Ordnungswidrigkeit nach Absatz 1 Nr. 2 und 3 Buchstabe a trifft in erster Linie den Erwerber eines Unternehmens oder einer Unternehmensbeteiligung bzw. den Übernehmer des Betriebs. Nach § 14 Abs. 1 des Ordnungswidrigkeitengesetzes kann dabei aber auch die Handlung des Veräußerers erfasst werden.

Führt ein Datenanbieter die Sensitivitätsprüfung vorsätzlich anhand falscher Kundendaten durch, so hat er die Sensitivität nicht richtig geprüft bzw. in Bezug auf die tatsächlichen Kundendaten gar nicht geprüft. Sind die angegebenen Kundendaten falsch und hätte der Datenanbieter dies erkennen können, so verletzt er ebenfalls die Prüfungspflicht und begeht eine fahrlässige Verletzung nach Nummer 6. In beiden Fällen können zudem Zweifel an der Zuverlässigkeit des Datenanbieters bestehen.

Tatbestände nach Absatz 2 sind nur bei Vorsatz erfüllt und betreffen Verstöße gegen Anzeige- und Auskunftspflichten. Sie sind mit einer Geldbuße von bis zu fünfundzwanzigtausend Euro bewehrt.

Der Bußgeldrahmen orientiert sich am Bußgeldrahmen des § 33 Abs. 6 AWG, da beide Gesetze den gleichen Schutzbereich haben. Es macht keinen Unterschied, ob Daten mit hohem Informationsgehalt verbreitet werden, weil eine Anfrage bedient wird oder weil ein Sensor ausgeführt wird, mittels dessen ein Gebietsfremder die Technik erwirbt, solche Daten selbst zu erzeugen.

Wird ein hochwertiges Erdfernerkundungssystem ohne Genehmigung betrieben, so können mangelnde Sicherheitsverfahren eine erhebliche (und dauerhafte) Gefährdung der Sicherheitsinteressen der Bundesrepublik Deutschland begründen. Dasselbe gilt für das Verbreiten von Daten ohne Zulassung und die Bedienung einer Anfrage ohne vorherige Durchführung einer Sensitivitätsprüfung oder die Bedienung einer sensitiven Anfrage ohne Erlaubnis. Die Erheblichkeit der Gefährdung und die Bedeutung der Schutzgüter bedingen die Möglichkeit der Bewehrung mit einer hohen Geldbuße. Dem Betreiber eines hochwertigen Erdfernerkundungssystems und dem Datenanbieter werden weitgehende Freiheiten zugestanden; sie unterliegen aber Dokumentations- und Prüfungspflichten. Missbraucht ein Betreiber oder

Anbieter diese Freiheit, so entfällt nicht nur die Möglichkeit der behördlichen Aufsicht, sondern es entsteht zudem ein kaum kontrollierbares Risiko für die Sicherheitsinteressen der Bundesrepublik Deutschland. Auch die Verletzung von Mitwirkungspflichten kann schwere Auswirkungen auf diese Sicherheitsinteressen haben, da die zuständige Behörde mangels Kenntnis nicht zeitnah auf eine mögliche Sicherheitsgefährdung reagieren kann. Diesen Wertungen zufolge wurde ein abgestuftes Bußgeldsystem gebildet.

Zuständig ist das Bundesministerium für Wirtschaft und Technologie nach der allgemeinen Regelung des § 35 ff. OWiG.

Zu § 29 (Straftaten)

Die Ordnungswidrigkeiten des § 28 Abs. 1 Nr. 1 bis 6 stellen Straftaten dar, wenn sie geeignet sind, die bezeichneten Rechtsgüter zu gefährden. Diese Eignung zur Gefährdung der Rechtsgüter (objektive Bedingung der Strafbarkeit) rechtfertigt eine Einordnung als kriminelles Unrecht, da es sich nicht mehr nur um Verstöße gegen formale Pflichten und insofern typisches Verwaltungsunrecht handelt. Die Rechtsgüter sind nicht nur hochrangig, sondern die Gefährdung kann auch erheblichen innen- und außenpolitischen Schaden nach sich ziehen. Der Strafrahmen orientiert sich am Strafrahmen des § 34 AWG, da beide Gesetze den gleichen Schutzbereich haben.

Zu § 30 (Auslandstaten Deutscher)

Die Regelung erweitert den strafrechtlichen Anwendungsbereich dieses Gesetzes entsprechend § 35 AWG und § 5 StGB. Dadurch wird eine Strafbarkeitslücke geschlossen.

Zu § 31 (Straf- und Bußgeldverfahren)

Absatz 1 dient der Einheitlichkeit der Rechtsprechung auf diesem Gebiet und erleichtert einen Gleichlauf der Rechtsprechung mit den Strafverfahren nach dem AWG. Absatz 2 gibt der zuständigen Behörde besondere Beteiligungsrechte. Diese Regelung macht die besondere Kompetenz der zuständigen Behörde auch im Strafverfahren nutzbar.

Zu § 32 (Änderung des Bundesverfassungsschutzgesetzes)

Das Bundesamt für Verfassungsschutz wirkt bei der Durchführung der einfachen Sicherheitsüberprüfung nach § 4 Abs. 2 und § 12 Abs. 2 mit. § 3 Abs. 2 BVerfSchG, der diese Mitwirkung regelt, ist daher zu ergänzen.

Zu § 33 (Änderung des Sicherheitsüberprüfungsgesetzes)

Nach § 4 Abs. 2 und § 12 Abs. 2 sind die zugangsberechtigten Personen einer Sicherheitsüberprüfung zu unterziehen. Damit auf diese das Sicherheitsüberprüfungsgesetz Anwendung finden kann, ist das SÜG zu ergänzen.

Die Ergänzung des § 3 Abs. 2 Satz 1 um Nr. 2 ist eine Folgeänderung zur Einführung des vorbeugenden personellen Sabotageschutzes in das Sicherheitsüberprüfungsgesetz, die im Terrorismusbekämpfungsgesetz versehentlich unterblieben war.

Zu § 34 (Übergangsregelung)

Die Übergangsregelung dient der Rechtssicherheit und dem Schutz der geschäftlichen Betätigung des Betreibers. Sie verhindert, dass mit dem Inkrafttreten des Gesetzes der Geschäftsbetrieb eingestellt werden muss, bis die erforderliche Genehmigung erteilt ist. Die Übergangsregelung knüpft an den Antrag an, der innerhalb von drei Monaten nach Inkrafttreten des Gesetzes zu stellen ist. Der Antrag muss den Anforderungen des § 25 entsprechen.

Entsprechendes gilt für die Zulassung von Datenanbietern.

Zu § 35 (Inkrafttreten)

Eine Rechtsverordnung kann erst ausgefertigt werden, wenn die Ermächtigungsnorm in Kraft getreten ist. Die Ermächtigungsnormen müssen daher alsbald nach Verkündigung in Kraft treten, um ein gemeinsames Inkrafttreten des übrigen Gesetzes mit den Rechtsverordnungen sicherzustellen.

Anlage 2

Stellungnahme des Bundesrates

Der Bundesrat hat in seiner 831. Sitzung am 9. März 2007 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Abs. 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. **Zu § 2 Abs. 1 Nr. 4**

   In § 2 Abs. 1 Nr. 4 sind die Wörter „Orbital- oder Transportsystem“ durch die Wörter „Transport- oder Orbitalsystem“ zu ersetzen.

   Begründung

   Von den für die Landesvermessung zuständigen Behörden der Länder der Bundesrepublik Deutschland werden als staatliche Kernaufgabe u. a. durch Erdfernerkundungssysteme mit flugzeuggetragenen Sensoren Luftbilder und daraus abgeleitete Produkte hergestellt und heute ohne Beschränkungen verbreitet.

   Die in § 2 SatDSiG-E vorgenommenen Begriffsbestimmungen zu den Begriffen „hochwertiges Erdfernerkundungssystem“, „Orbital- oder Transportsystem“ und „Daten mit besonders hohem Informationsgehalt“ schließen hochauflösende Luftbilder mit ein.

   Aus der Begründung zu § 2 Abs. 1 SatDSiG-E geht aber hervor, dass nur Orbitalsysteme und Transportsysteme gemeint sind, die eine Erdumlaufbahn erreichen. Durch eine Umstellung des Begriffspaars muss dies klargestellt werden.

2. Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren sicherzustellen, dass die Bestimmungen zur anfragebezogenen Sensitivitätsprüfung eine softwaregestützte und damit automatisierbare Prüfung („EDV-Prüf-Routine“) erlauben und hierzu die Möglichkeit einer behördlichen Zertifizierung der Prüfroutinen zu schaffen oder behördlich zertifizierte Prüfroutinen bereitzustellen.

   Begründung

   Der Bundesrat erkennt bei dem Betrieb von hochwertigen Erdfernerkundungssystemen und in der Verbreitung von hiermit erzeugten hochwertigen Erdfernerkundungsdaten ein erhebliches wirtschaftliches Potenzial. Der Bundesrat anerkennt die mögliche lokale, personelle und/oder temporale Sensitivität der hochwertigen Erdfernerkundungsdaten und die hieraus resultierende Verantwortung bei der Verbreitung dieser Daten. Die aus der Verbreitung der hochwertigen Erdfernerkundungsdaten resultierenden Rechtsverbindlichkeiten und Rechtsfolgen sollen in der Verantwortung der öffentlichen Hand liegen.

   Dabei ist dem Umstand Rechnung zu tragen, dass die Sensitivität der Daten nicht pauschal festgestellt werden kann, im Einzelfall von der beantragenden Stelle und/oder den angefragten Daten abhängt und somit antragsbezogen zu prüfen ist.

   Die Verwendung einer zertifizierten und damit zugelassenen Software zur Sensitivitätsprüfung bei Antragseingang bei den Datenanbietern würde die öffentliche Hand in der Verantwortung über die Verbreitung hochwertiger Erdfernerkundungsdaten belassen und die Daten verbreitenden Stellen von der Wahrnehmung hoheitlicher Aufgaben entbinden.

   Die „EDV-Prüf-Routine“ ist wahlweise durch die zuständige Behörde oder durch die Daten verbreitende Stelle zu entwickeln. In beiden Fällen ist die „EDV-Prüf-Routine“ durch die zuständige Behörde zu zertifizieren.

Anlage 3

Gegenäußerung der Bundesregierung

Die Bundesregierung nimmt zu den Vorschlägen des Bundesrates wie folgt Stellung:

Zu Nummer 1

Zu § 2 Abs. 1 Nr. 4 schlägt der Bundesrat vor, die Wörter „Orbital- oder Transportsystem“ durch die Wörter „Transport- oder Orbitalsystem“ zu ersetzen.

Mit der vorgeschlagenen Umstellung soll klargestellt werden, dass der Anwendungsbereich des Satellitendatensicherheitsgesetzes nur Daten von raumgestützten Erdfernerkundungssystemen (d. h. im Wesentlichen Satelliten), nicht jedoch Luftbilder oder Daten von flugzeuggestützten Sensoren umfasst.

Es ist die Intention der Bundesregierung, mit dem Entwurf zum Satellitendatensicherheitsgesetz nur raumgestützte Erdfernerkundungssysteme zu erfassen. Die Bundesregierung ist der Ansicht, dass dieses Ziel bereits durch den vorgelegten Entwurf in ausreichender Weise sichergestellt war.

Die Bundesregierung stimmt dem Vorschlag zu.

Zu Nummer 2

Der Bundesratsbeschluss bezieht sich auf die praktische Ausgestaltung eines im Gesetzentwurf vorgesehenen Prüfverfahrens, das vom Datenanbieter durchzuführen ist (§ 17 Abs. 2). Hierzu bittet der Bundesrat im weiteren Gesetzgebungsverfahren sicherzustellen, dass die Bestimmungen zur anfragebezogenen Sensitivitätsprüfung eine softwaregestützte und damit automatisierbare Prüfung („EDV-Prüf-Routine“) erlauben, und hierzu die Möglichkeit einer behördlichen Zertifizierung der Prüfroutinen zu schaffen oder behördlich zertifizierte Prüfroutinen bereitzustellen.

Die Bundesregierung begrüßt den Vorschlag und wird prüfen, wie dies in der Ausgestaltung der Verfahren, beispielsweise durch Berücksichtigung in der Rechtsverordnung nach § 17 Abs. 2, 3 SatDSiG-E, im Rahmen der vorhandenen Finanzierungsspielräume umgesetzt werden kann.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333